**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

| | |
|---|---|
| Applicants: | Satoshi KITANI et al. |
| International Application No.: | PCT/JP04/004909 |
| International Filing Date: | April 5, 2004 |
| For: | INFORMATION-RECORDING MEDIUM DRIVE |

745 Fifth Avenue
New York, NY 10151

**EXPRESS MAIL**

Mailing Label Number: EV206809556US

Date of Deposit: December 10, 2004

I hereby certify that this paper or fee is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" Service under 37 CFR 1.10 on the date indicated above and is addressed to Mail Stop PCT, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Barnet Shindhman
(Typed or printed name of person mailing paper or fee)

(Signature of person mailing paper or fee)

**CLAIM OF PRIORITY UNDER 37 C.F.R. § 1.78(a)(2)**

Mail Stop PCT
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Pursuant to 35 U.S.C. 119, this application is entitled to a claim of priority to Japan Application No. 2003-107571 filed 11 April 2003.

Respectfully submitted,

FROMMER LAWRENCE & HAUG LLP
Attorneys for Applicants

By: _____
William S. Frommer
Reg. No. 25,506
Tel. (212) 588-0800

PCT/JP2004/004909
10517783

# 日本国特許庁
JAPAN PATENT OFFICE

05. 4. 2004

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年　４月１１日

出願番号
Application Number: 特願２００３－１０７５７１
[ST. 10/C]: [ＪＰ２００３－１０７５７１]



出願人
Applicant(s): ソニー株式会社

**PRIORITY DOCUMENT**
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

２００４年　５月１４日

特許庁長官
Commissioner,
Japan Patent Office
今井康夫

出証番号　出証特２００４－３０４０１６４

【書類名】　特許願
【整理番号】　0390293210
【提出日】　平成15年 4月11日
【あて先】　特許庁長官殿
【国際特許分類】　H04L 9/16
【発明者】
【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内
【氏名】　木谷　聡
【発明者】
【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内
【氏名】　米満　潤
【発明者】
【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内
【氏名】　村松　克美
【発明者】
【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内
【氏名】　浅野　智之
【発明者】
【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内
【氏名】　高島　芳和
【特許出願人】
【識別番号】　000002185
【氏名又は名称】　ソニー株式会社

【代理人】
【識別番号】　100093241
【弁理士】
【氏名又は名称】　宮田　正昭
【電話番号】　03-5541-7577
【選任した代理人】
【識別番号】　100101801
【弁理士】
【氏名又は名称】　山田　英治
【電話番号】　03-5541-7577
【選任した代理人】
【識別番号】　100086531
【弁理士】
【氏名又は名称】　澤田　俊夫
【電話番号】　03-5541-7577
【手数料の表示】
【予納台帳番号】　048747
【納付金額】　21,000円
【提出物件の目録】
【物件名】　明細書　1
【物件名】　図面　1
【物件名】　要約書　1
【包括委任状番号】　9904833
【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　情報処理装置、情報記録媒体ドライブ装置、情報記録媒体、および情報処理方法、並びにコンピュータ・プログラム

【特許請求の範囲】

【請求項１】

情報記録媒体に格納された暗号化データの復号処理を実行する情報処理装置であり、

情報記録媒体に格納された暗号化データを構成する暗号化処理単位毎に設定された鍵生成情報としての第１シードに基づいて第１ブロックキーＫｂ１を生成し、生成した第１ブロックキーＫｂ１に基づいて情報記録媒体に格納された暗号化第２シードの復号処理を実行して第２シードを取得し、取得した第２シードに基づいて第２ブロックキーＫｂ２を生成し、生成した第２ブロックキーＫｂ２に基づく復号処理により前記情報記録媒体に格納された暗号化データの復号処理を実行する暗号処理手段を有することを特徴とする情報処理装置。

【請求項２】

前記情報処理装置は、

マスターキー生成情報を格納した記憶手段を有し、

前記暗号処理手段は、

前記マスターキー生成情報に基づいてマスターキーを生成し、該生成したマスターキーと前記情報記録媒体からの読み出し情報とに基づいて、２つの記録キーＫ１，Ｋ２を生成し、生成した第１記録キーＫ１と前記第１シード情報とに基づく暗号処理により前記第１ブロックキーＫｂ１を生成し、生成した第１ブロックキーＫｂ１に基づいて情報記録媒体に格納された暗号化第２シードの復号処理を実行して第２シードを取得し、取得した第２シードと第２記録キーＫ２とに基づく暗号処理により前記第２ブロックキーＫｂ２を生成し、生成した第２ブロックキーＫｂ２に基づく復号処理により前記情報記録媒体に格納された暗号化データの復号処理を実行する構成であることを特徴とする請求項１に記載の情報処理装置。

【請求項３】

前記暗号処理手段は、

前記マスターキーと、前記情報記録媒体からの読み出し情報であるディスクＩＤ、および前記情報記録媒体に記録された２つのタイトルキーに基づいて第１タイトル固有キーおよび第２タイトル固有キーを生成し、さらに、

前記第１タイトル固有キーと、前記情報記録媒体からの第１読み出し情報とに基づく暗号処理により前記第１記録キーＫ１を生成し、

前記第２タイトル固有キーと、前記情報記録媒体からの第２読み出し情報とに基づく暗号処理により前記第２記録キーＫ２を生成する構成であることを特徴とする請求項２に記載の情報処理装置。

【請求項４】

前記暗号処理手段は、

前記マスターキーと、前記情報記録媒体からの読み出し情報であるディスクＩＤ、および前記情報記録媒体に記録された１つのキーシード情報に基づいて第１タイトル固有キーおよび第２タイトル固有キーを生成し、さらに、

前記第１タイトル固有キーと、前記情報記録媒体からの第１読み出し情報とに基づく暗号処理により前記第１記録キーＫ１を生成し、

前記第２タイトル固有キーと、前記情報記録媒体からの第２読み出し情報とに基づく暗号処理により前記第２記録キーＫ２を生成する構成であることを特徴とする請求項２に記載の情報処理装置。

【請求項５】

情報記録媒体に格納された暗号化データの読み取りおよび外部出力を実行する情報記録媒体ドライブ装置であり、

情報記録媒体に格納された暗号化データの出力先装置との認証処理を実行しセッションキーＫｓを生成する認証処理部と、

情報記録媒体に格納された暗号化データを構成する暗号化処理単位毎に設定された鍵生成情報としての第１シードに基づいて第１ブロックキーＫｂ１を生成し、生成した第１ブロックキーＫｂ１に基づいて情報記録媒体に格納された暗号化第２シードの復号処理を実行して第２シードを取得し、前記セッションキーＫｓに基づいて前記第２シードを含むデータの暗号化処理を実行し出力用暗号化情報

を生成する暗号処理手段とを有し、

前記セッションキーＫｓに基づいて暗号化された第２シードを含む出力用暗号化情報をインタフェースを介して出力する構成を有することを特徴とする情報記録媒体ドライブ装置。

【請求項６】

前記暗号処理手段は、

情報記録媒体ドライブ装置の保有するマスターキー生成情報に基づいて生成したマスターキーと、前記情報記録媒体からの読み出し情報とに基づいて、２つの記録キーＫ１，Ｋ２を生成し、生成した第１記録キーＫ１と前記第１シード情報とに基づく暗号処理により前記第１ブロックキーＫｂ１を生成し、生成した第１ブロックキーＫｂ１に基づいて情報記録媒体に格納された暗号化第２シードの復号処理を実行して第２シードを取得し、取得した第２シードと第２記録キーＫ２とを含むデータを前記セッションキーＫｓに基づいて暗号化して出力用暗号化情報を生成し、

前記第２シードと第２記録キーＫ２とを含む前記出力用暗号化情報をインタフェースを介して出力する構成を有することを特徴とする請求項５に記載の情報記録媒体ドライブ装置。

【請求項７】

データ入力インタフェースを介して入力する暗号データの復号処理を実行する情報処理装置であり、

前記暗号データの出力装置との認証処理を実行しセッションキーＫｓを生成する認証処理部と、

前記データ入力インタフェースを介して入力する暗号化情報を前記セッションキーに基づく復号処理により鍵生成情報としてのシード情報および記録キーを取得し、前記シード情報および記録キーに基づく暗号処理により暗号データの復号キーとしてのブロックキーを生成し、該ブロックキーに基づく暗号データの復号処理を実行する暗号処理部と、

を有することを特徴とする情報処理装置。

【請求項８】

情報記録媒体に格納された暗号化データの読み取りおよび外部出力を実行する情報記録媒体ドライブ装置であり、

情報記録媒体に格納された暗号化データの出力先装置との認証処理を実行しセッションキーＫｓを生成する認証処理部と、

情報記録媒体に格納された暗号化データを構成する暗号化処理単位毎に設定された鍵生成情報としてのシードに基づいてブロックキーを生成し、生成したブロックキーに基づいて情報記録媒体に格納された暗号化データの復号処理を実行して復号データを取得し、前記セッションキーＫｓに基づいて前記復号データの暗号化処理を実行し出力用暗号化情報を生成する暗号処理手段とを有し、

前記セッションキーＫｓに基づいて暗号化された出力用暗号化情報をインタフェースを介して出力する構成を有することを特徴とする情報記録媒体ドライブ装置。

【請求項９】

暗号化データを格納した情報記録媒体であり、

暗号化データを構成する暗号化処理単位毎に設定された鍵生成情報としての第１シードと、

前記第１シードに基づいて生成される第１ブロックキーＫｂ１に基づいて暗号化された鍵生成情報としての暗号化第２シードと、

前記第２シードに基づいて生成される第２ブロックキーＫｂ１に基づいて暗号化された暗号化コンテンツと、

を格納した構成を有することを特徴とする情報記録媒体。

【請求項１０】

前記第１シードは、前記暗号化処理単位毎に設定された制御情報内に格納され、

前記第２シードは、前記制御情報外のユーザデータ領域に暗号化されて格納された構成であることを特徴とする請求項９に記載の情報記録媒体。

【請求項１１】

前記第１シードは、ユーザデータ領域に非暗号化データとして格納され、

前記第２シードは、ユーザデータ領域に暗号化データとして格納された構成で

あることを特徴とする請求項９に記載の情報記録媒体。

【請求項１２】

前記暗号化データは、トランスポートストリームパケットから構成され、

前記第１シードは、複数のトランスポートストリームパケットに対応する制御情報内に格納され、前記第２シードは、前記制御情報外のユーザデータ領域のトランスポートストリームパケット内に暗号化されて格納された構成であることを特徴とする請求項９に記載の情報記録媒体。

【請求項１３】

前記暗号化データは、トランスポートストリームパケットから構成され、

前記第１シードは、ユーザデータ領域のトランスポートストリームパケット内に非暗号化データとして格納され、

前記第２シードは、ユーザデータ領域のトランスポートストリームパケット内に暗号化されて格納された構成であることを特徴とする請求項９に記載の情報記録媒体。

【請求項１４】

情報記録媒体に格納された暗号化データの復号処理を実行する情報処理方法であり、

情報記録媒体に格納された暗号化データを構成する暗号化処理単位毎に設定された鍵生成情報としての第１シードに基づいて第１ブロックキーＫｂ１を生成するステップと、

生成した第１ブロックキーＫｂ１に基づいて情報記録媒体に格納された暗号化第２シードの復号処理を実行して第２シードを取得し、取得した第２シードに基づいて第２ブロックキーＫｂ２を生成するステップと、

生成した第２ブロックキーＫｂ２に基づく復号処理により前記情報記録媒体に格納された暗号化データの復号処理を実行するステップと、

を有することを特徴とする情報処理方法。

【請求項１５】

前記情報処理方法は、さらに、

記憶手段から読み出したマスターキー生成情報に基づいて生成したマスターキ

ーと、前記情報記録媒体からの読み出し情報とに基づいて、２つの記録キーＫ１，Ｋ２を生成するステップを有し、

生成した第１記録キーＫ１と前記第１シード情報とに基づく暗号処理により前記第１ブロックキーＫｂ１を生成し、生成した第１ブロックキーＫｂ１に基づいて情報記録媒体に格納された暗号化第２シードの復号処理を実行して第２シードを取得し、取得した第２シードと第２記録キーＫ２とに基づく暗号処理により前記第２ブロックキーＫｂ２を生成し、生成した第２ブロックキーＫｂ２に基づく復号処理により前記情報記録媒体に格納された暗号化データの復号処理を実行することを特徴とする請求項１４に記載の情報処理方法。

【請求項１６】

前記情報処理方法は、

前記マスターキーと、前記情報記録媒体からの読み出し情報であるディスクＩＤ、および前記情報記録媒体に記録された２つのタイトルキーに基づいて第１タイトル固有キーおよび第２タイトル固有キーを生成し、さらに、

前記第１タイトル固有キーと、前記情報記録媒体からの第１読み出し情報とに基づく暗号処理により前記第１記録キーＫ１を生成し、

前記第２タイトル固有キーと、前記情報記録媒体からの第２読み出し情報とに基づく暗号処理により前記第２記録キーＫ２を生成するステップを有することを特徴とする請求項１５に記載の情報処理方法。

【請求項１７】

前記情報処理方法は、

前記マスターキーと、前記情報記録媒体からの読み出し情報であるディスクＩＤ、および前記情報記録媒体に記録された１つのキーシード情報に基づいて第１タイトル固有キーおよび第２タイトル固有キーを生成し、さらに、

前記第１タイトル固有キーと、前記情報記録媒体からの第１読み出し情報とに基づく暗号処理により前記第１記録キーＫ１を生成し、

前記第２タイトル固有キーと、前記情報記録媒体からの第２読み出し情報とに基づく暗号処理により前記第２記録キーＫ２を生成するステップを有することを特徴とする請求項１５に記載の情報処理方法。

【請求項１８】

情報記録媒体に格納された暗号化データの読み取りおよび外部出力を実行する情報処理方法であり、

情報記録媒体に格納された暗号化データの出力先装置との認証処理を実行しセッションキーＫｓを生成する認証処理ステップと、

情報記録媒体に格納された暗号化データを構成する暗号化処理単位毎に設定された鍵生成情報としての第１シードに基づいて第１ブロックキーＫｂ１を生成するステップと、

生成した第１ブロックキーＫｂ１に基づいて情報記録媒体に格納された暗号化第２シードの復号処理を実行して第２シードを取得し、前記セッションキーＫｓに基づいて前記第２シードを含むデータの暗号化処理を実行し出力用暗号化情報を生成するステップと、

前記セッションキーＫｓに基づいて暗号化された第２シードを含む出力用暗号化情報をインタフェースを介して出力するステップと、

を有することを特徴とする情報処理方法。

【請求項１９】

前記情報処理方法は、

情報記録媒体ドライブ装置の保有するマスターキー生成情報に基づいて生成したマスターキーと、前記情報記録媒体からの読み出し情報とに基づいて、２つの記録キーＫ１，Ｋ２を生成し、生成した第１記録キーＫ１と前記第１シード情報とに基づく暗号処理により前記第１ブロックキーＫｂ１を生成し、生成した第１ブロックキーＫｂ１に基づいて情報記録媒体に格納された暗号化第２シードの復号処理を実行して第２シードを取得し、取得した第２シードと第２記録キーＫ２とを含むデータを前記セッションキーＫｓに基づいて暗号化して出力用暗号化情報を生成し、

前記第２シードと第２記録キーＫ２とを含む前記出力用暗号化情報をインタフェースを介して出力することを特徴とする請求項１８に記載の情報処理方法。

【請求項２０】

データ入力インタフェースを介して入力する暗号データの復号処理を実行する

情報処理方法であり、

前記暗号データの出力装置との認証処理を実行しセッションキーＫｓを生成する認証処理ステップと、

前記データ入力インタフェースを介して入力する暗号化情報を前記セッションキーに基づく復号処理により鍵生成情報としてのシード情報および記録キーを取得し、前記シード情報および記録キーに基づく暗号処理により暗号データの復号キーとしてのブロックキーを生成し、該ブロックキーに基づく暗号データの復号処理を実行する暗号処理ステップと、

を有することを特徴とする情報処理方法。

【請求項２１】

情報記録媒体に格納された暗号化データの読み取りおよび外部出力を実行する情報処理方法であり、

情報記録媒体に格納された暗号化データの出力先装置との認証処理を実行しセッションキーＫｓを生成する認証処理ステップと、

情報記録媒体に格納された暗号化データを構成する暗号化処理単位毎に設定された鍵生成情報としてのシードに基づいてブロックキーを生成し、生成したブロックキーに基づいて情報記録媒体に格納された暗号化データの復号処理を実行して復号データを取得し、前記セッションキーＫｓに基づいて前記復号データの暗号化処理を実行し出力用暗号化情報を生成する暗号処理ステップと、

前記セッションキーＫｓに基づいて暗号化された出力用暗号化情報をインタフェースを介して出力するステップと、

を有することを特徴とする情報処理方法。

【請求項２２】

情報記録媒体に格納された暗号化データの復号処理を実行するコンピュータ・プログラムであり、

情報記録媒体に格納された暗号化データを構成する暗号化処理単位毎に設定された鍵生成情報としての第１シードに基づいて第１ブロックキーＫｂ１を生成するステップと、

生成した第１ブロックキーＫｂ１に基づいて情報記録媒体に格納された暗号化

第２シードの復号処理を実行して第２シードを取得し、取得した第２シードに基づいて第２ブロックキーＫｂ２を生成するステップと、

生成した第２ブロックキーＫｂ２に基づく復号処理により前記情報記録媒体に格納された暗号化データの復号処理を実行するステップと、

を有することを特徴とするコンピュータ・プログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、情報処理装置、情報記録媒体ドライブ装置、情報記録媒体、および情報処理方法、並びにコンピュータ・プログラムに関する。詳細には、情報記録媒体を利用したデータ記録再生処理における不正なコンテンツ利用の防止を実現する情報処理装置、情報記録媒体ドライブ装置、情報記録媒体、および情報処理方法、並びにコンピュータ・プログラムに関する。

【０００２】

【従来の技術】

昨今、音楽等のオーディオデータ、映画等の画像データ、ゲームプログラム、各種アプリケーションプログラム等、様々なソフトウエアデータ（以下、これらをコンテンツ（Content）と呼ぶ）が、インターネット等のネットワークを介して、あるいはＣＤ(Compact Disc)、ＤＶＤ(Digital Versatile Disk)、ＭＤ(Mini Disk)等の情報記録媒体（メディア）を介して流通している。これらの流通コンテンツは、ユーザの所有するＰＣ（Personal Computer）、ＣＤプレーヤ、ＤＶＤプレーヤ、ＭＤプレーヤ等の再生装置、あるいはゲーム機器等において再生され利用される。

【０００３】

音楽データ、画像データ等、多くのコンテンツは、一般的にその作成者あるいは販売者に頒布権等が保有されている。従って、これらのコンテンツの配布に際しては、一定の利用制限、すなわち、正規なユーザに対してのみ、コンテンツの利用を許諾し、許可のない複製等が行われないようにする構成をとるのが一般的となっている。

【０００４】

特に、近年においては、情報をデジタル的に記録する記録装置や記録媒体が普及しつつある。このようなデジタル記録装置および記録媒体によれば、例えば画像や音声を劣化させることなく記録、再生を繰り返すことが可能であり、不正コピーコンテンツのインターネットを介した配信や、コンテンツをＣＤ－Ｒ等にコピーした、いわゆる海賊版ディスクが大量に流通しているという問題がある。

【０００５】

特に、近年開発されたＤＶＤ等の大容量型記録媒体は、１枚の媒体に例えば映画１本分の大量のデータをデジタル情報として記録することが可能である。このように映像情報等をデジタル情報として記録することが可能となってくると不正コピーを防止して著作権者の保護を図ることが益々重要な課題となっている。

【０００６】

デジタル記録再生を行う記録装置やデジタル記録媒体によれば、画像や音声を劣化させることなく記録、再生を繰り返すことができる。このようにデジタルデータは画質や音質を維持したまま何度もコピーを繰り返し実行することができるため、コピーが違法に行われた記録媒体が市場に流通すると、音楽、映画等各種コンテンツの著作権者、あるいは正当な販売権者等の利益が害されることになる。昨今では、このようなデジタルデータの不正なコピーを防ぐため、デジタル記録装置および記録媒体に違法なコピーを防止するための様々な技術が実用化されている。

【０００７】

例えば、ＤＶＤプレーヤでは、コンテンツ・スクランブルシステム（Ｃｏｎｔｅｎｔ　Ｓｃｒａｍｂｌｅ　Ｓｙｓｔｅｍ）が採用されている。コンテンツ・スクランブルシステムでは、ＤＶＤ－ＲＯＭ(Read Only Memory)に、ビデオデータやオーディオデータ等が暗号化されて記録されており、その暗号化されたデータを復号するのに用いる鍵が、ライセンスを受けたＤＶＤプレーヤに与えられる。ライセンスは、不正コピーを行わない等の所定の動作規定に従うように設計されたＤＶＤプレーヤに対して与えられる。従って、ライセンスを受けたＤＶＤプレーヤでは、与えられたキーを利用して、ＤＶＤ－ＲＯＭに記録された暗号化デー

タを復号することにより、ＤＶＤ－ＲＯＭから画像や音声を再生することができる。

【０００８】

一方、ライセンスを受けていないＤＶＤプレーヤは、暗号化されたデータを復号するための鍵を有していないため、ＤＶＤ－ＲＯＭに記録された暗号化データの復号を行うことができない。このように、コンテンツ・スクランブルシステム構成では、ライセンス時に要求される条件を満たしていないＤＶＤプレーヤは、デジタルデータを記録したＤＶＤ－ＲＯＭの再生を行なえないことになり、不正コピーが防止されるようになっている。

【０００９】

しかしながら、ＤＶＤ－ＲＯＭで採用されているコンテンツ・スクランブルシステムは、ユーザによるデータの書き込みが不可能な記録媒体を対象としており、ユーザによるデータの書き込みが可能な記録媒体への適用については考慮されていない。

【００１０】

即ち、データの書き込みが可能な記録媒体に記録されたデータが暗号化されていても、その暗号化されたデータを、そのまま全部、ＲＡＭメディアにコピーした場合には、ライセンスを受けた正当な装置で再生可能な、いわゆる海賊版を作成することができてしまう。

【００１１】

さらに、ＣＳＳの暗号を破るソフトウェアプログラム、例えばＤｅＣＳＳソフトウェアがインターネット上で配布されており、このプログラムを適用することで、ＤＶＤ　Ｖｉｄｅｏの暗号を解いて平文の状態で記録型ＤＶＤへ書き込むことが可能になっている。ＤｅＣＳＳが出現した背景は、本来暗号化が義務付けられているはずのＣＳＳ復号用の鍵データを暗号化しないまま設計されたＤＶＤプレーヤー・ソフトウェアがリバースエンジニアされて鍵データが解読されたことであり、解読された鍵データから連鎖的にＣＳＳアルゴリズム全体が解読されたという経緯である。

【００１２】

鍵データを含む著作権保護技術実行プログラムをＰＣ上で実行されるアプリケーションプログラムへ実装する際には、著作権保護技術の解析を防ぐため耐タンパー性を持たせるのが一般的であるが、対タンパー性の強度を示す指標は無く、そのためどれほどリバースエンジニアリングへの対応を行うかは個々のインプレメンターの判断や実力に委ねられているのが実情であり、ＣＳＳの場合には結果として破られてしまい、不正なコピーコンテンツの氾濫を招く結果となっている。

【００１３】

ＣＳＳ以外にも、ＤＶＤ規格で採用されている著作権保護技術(コピーコントロール技術）として、ＣＰＰＭ（Content Protection for Prerecorded Media）とＣＰＲＭ（Content Protection for Recordable Media）がある。ＣＰＰＭは、再生専用のメディア（Prerecorded Media）用に開発されたコピーコントロール技術であり、ＣＰＲＭは、記録可能なメディア（Recordable Media）用に開発されたコピーコントロール技術である。これらは、メディア（例えばディスク）側にメディアキーブロックと呼ばれる鍵情報を格納し、一方、再生装置、ＰＣ等、デバイス側にデバイスキーを格納し、これらの鍵の組み合わせにより、コピーコントロールを行うものである。

【００１４】

しかし、このようなＣＰＲＭや、ＣＰＰＭにおいても、デバイスとしてのＰＣやメディアとしてのディスク内に格納された鍵情報の漏洩の危険性を解消するといった根本的な問題解決を図る技術についての提案はなく、ＣＰＲＭや、ＣＰＰＭにおいても、鍵の漏洩によってコピーコントロールシステムが崩壊する危険性を常に有しているのが現状である。

【００１５】

なお、コンテンツの不正利用を防止する技術として、本出願人は、例えば特許文献１および特許文献２において、記録媒体に格納するコンテンツのデータブロック毎に異なる鍵を適用した暗号処理技術を提案した。すなわち、データブロック毎の鍵生成情報としてシードを設定し、ブロック毎に設定したシードを暗号鍵の生成に適用する構成により、従来の１つの鍵のみによるコンテンツ暗号化を複

雑化して、暗号アルゴリズムの解読困難性を高めたものである。

【００１６】

しかし、上述の構成において、データブロック毎の鍵生成情報としてシードは、記録媒体に格納された情報そのものを使用したものであり、前述のＣＳＳと同様の経緯で鍵データが解読され、解読された鍵データとデータブロック毎に異なるシードからブロックキーが導かれることによりコンテンツの漏洩を引き起こす懸念が皆無とはいえない。

【００１７】

【特許文献１】

特許公開２００１－３５１３２４号公報

【特許文献２】

特許公開２００２－２３６６２２号公報

【００１８】

【発明が解決しようとする課題】

本発明は、上述の従来技術における問題点に鑑みてなされたものであり、ＤＶＤ、ＣＤ等の各種情報記録媒体に格納したコンテンツを再生装置、ＰＣ（パーソナルコンピュータ）において利用する構成において、記録媒体に格納するコンテンツの暗号化に適用する鍵情報の漏洩をより困難とし、鍵解読、暗号アルゴリズムの解読の困難性を高めることを実現した情報処理装置、情報記録媒体ドライブ装置、情報記録媒体、および情報処理方法、並びにコンピュータ・プログラムを提供することを目的とする。

【００１９】

【課題を解決するための手段】

本発明の第１の側面は、

情報記録媒体に格納された暗号化データの復号処理を実行する情報処理装置であり、

情報記録媒体に格納された暗号化データを構成する暗号化処理単位毎に設定された鍵生成情報としての第１シードに基づいて第１ブロックキーＫｂ１を生成し、生成した第１ブロックキーＫｂ１に基づいて情報記録媒体に格納された暗号化

第２シードの復号処理を実行して第２シードを取得し、取得した第２シードに基づいて第２ブロックキーＫｂ２を生成し、生成した第２ブロックキーＫｂ２に基づく復号処理により前記情報記録媒体に格納された暗号化データの復号処理を実行する暗号処理手段を有することを特徴とする情報処理装置にある。

【００２０】

さらに、本発明の情報処理装置の一実施態様において、前記情報処理装置は、マスターキー生成情報を格納した記憶手段を有し、前記暗号処理手段は、前記マスターキー生成情報に基づいてマスターキーを生成し、該生成したマスターキーと前記情報記録媒体からの読み出し情報とに基づいて、２つの記録キーＫ１，Ｋ２を生成し、生成した第１記録キーＫ１と前記第１シード情報とに基づく暗号処理により前記第１ブロックキーＫｂ１を生成し、生成した第１ブロックキーＫｂ１に基づいて情報記録媒体に格納された暗号化第２シードの復号処理を実行して第２シードを取得し、取得した第２シードと第２記録キーＫ２とに基づく暗号処理により前記第２ブロックキーＫｂ２を生成し、生成した第２ブロックキーＫｂ２に基づく復号処理により前記情報記録媒体に格納された暗号化データの復号処理を実行する構成であることを特徴とする。

【００２１】

さらに、本発明の情報処理装置の一実施態様において、前記暗号処理手段は、前記マスターキーと、前記情報記録媒体からの読み出し情報であるディスクＩＤ、および前記情報記録媒体に記録された２つのタイトルキーに基づいて第１タイトル固有キーおよび第２タイトル固有キーを生成し、さらに、前記第１タイトル固有キーと、前記情報記録媒体からの第１読み出し情報とに基づく暗号処理により前記第１記録キーＫ１を生成し、前記第２タイトル固有キーと、前記情報記録媒体からの第２読み出し情報とに基づく暗号処理により前記第２記録キーＫ２を生成する構成であることを特徴とする。

【００２２】

さらに、本発明の情報処理装置の一実施態様において、前記暗号処理手段は、前記マスターキーと、前記情報記録媒体からの読み出し情報であるディスクＩＤ、および前記情報記録媒体に記録された１つのキーシード情報に基づいて第１タ

イトル固有キーおよび第２タイトル固有キーを生成し、さらに、前記第１タイトル固有キーと、前記情報記録媒体からの第１読み出し情報とに基づく暗号処理により前記第１記録キーＫ１を生成し、前記第２タイトル固有キーと、前記情報記録媒体からの第２読み出し情報とに基づく暗号処理により前記第２記録キーＫ２を生成する構成であることを特徴とする。

【００２３】

さらに、本発明の第２の側面は、

情報記録媒体に格納された暗号化データの読み取りおよび外部出力を実行する情報記録媒体ドライブ装置であり、

情報記録媒体に格納された暗号化データの出力先装置との認証処理を実行しセッションキーＫｓを生成する認証処理部と、

情報記録媒体に格納された暗号化データを構成する暗号化処理単位毎に設定された鍵生成情報としての第１シードに基づいて第１ブロックキーＫｂ１を生成し、生成した第１ブロックキーＫｂ１に基づいて情報記録媒体に格納された暗号化第２シードの復号処理を実行して第２シードを取得し、前記セッションキーＫｓに基づいて前記第２シードを含むデータの暗号化処理を実行し出力用暗号化情報を生成する暗号処理手段とを有し、

前記セッションキーＫｓに基づいて暗号化された第２シードを含む出力用暗号化情報をインタフェースを介して出力する構成を有することを特徴とする情報記録媒体ドライブ装置にある。

【００２４】

さらに、本発明の情報記録媒体ドライブ装置の一実施態様において、前記暗号処理手段は、情報記録媒体ドライブ装置の保有するマスターキー生成情報に基づいて生成したマスターキーと、前記情報記録媒体からの読み出し情報とに基づいて、２つの記録キーＫ１，Ｋ２を生成し、生成した第１記録キーＫ１と前記第１シード情報とに基づく暗号処理により前記第１ブロックキーＫｂ１を生成し、生成した第１ブロックキーＫｂ１に基づいて情報記録媒体に格納された暗号化第２シードの復号処理を実行して第２シードを取得し、取得した第２シードと第２記録キーＫ２とを含むデータを前記セッションキーＫｓに基づいて暗号化して出力

用暗号化情報を生成し、前記第２シードと第２記録キーＫ２とを含む前記出力用暗号化情報をインタフェースを介して出力する構成を有することを特徴とする。

【００２５】

さらに、本発明の第３の側面は、

データ入力インタフェースを介して入力する暗号データの復号処理を実行する情報処理装置であり、

前記暗号データの出力装置との認証処理を実行しセッションキーＫｓを生成する認証処理部と、

前記データ入力インタフェースを介して入力する暗号化情報を前記セッションキーに基づく復号処理により鍵生成情報としてのシード情報および記録キーを取得し、前記シード情報および記録キーに基づく暗号処理により暗号データの復号キーとしてのブロックキーを生成し、該ブロックキーに基づく暗号データの復号処理を実行する暗号処理部と、

を有することを特徴とする情報処理装置にある。

【００２６】

さらに、本発明の第４の側面は、

情報記録媒体に格納された暗号化データの読み取りおよび外部出力を実行する情報記録媒体ドライブ装置であり、

情報記録媒体に格納された暗号化データの出力先装置との認証処理を実行しセッションキーＫｓを生成する認証処理部と、

情報記録媒体に格納された暗号化データを構成する暗号化処理単位毎に設定された鍵生成情報としてのシードに基づいてブロックキーを生成し、生成したブロックキーに基づいて情報記録媒体に格納された暗号化データの復号処理を実行して復号データを取得し、前記セッションキーＫｓに基づいて前記復号データの暗号化処理を実行し出力用暗号化情報を生成する暗号処理手段とを有し、

前記セッションキーＫｓに基づいて暗号化された出力用暗号化情報をインタフェースを介して出力する構成を有することを特徴とする情報記録媒体ドライブ装置にある。

【００２７】

さらに、本発明の第５の側面は、

暗号化データを格納した情報記録媒体であり、

暗号化データを構成する暗号化処理単位毎に設定された鍵生成情報としての第１シードと、

前記第１シードに基づいて生成される第１ブロックキーＫｂ１に基づいて暗号化された鍵生成情報としての暗号化第２シードと、

前記第２シードに基づいて生成される第２ブロックキーＫｂ１に基づいて暗号化された暗号化コンテンツと、

を格納した構成を有することを特徴とする情報記録媒体にある。

【００２８】

さらに、本発明の情報記録媒体の一実施態様において、前記第１シードは、前記暗号化処理単位毎に設定された制御情報内に格納され、前記第２シードは、前記制御情報外のユーザデータ領域に暗号化されて格納された構成であることを特徴とする。

【００２９】

さらに、本発明の情報記録媒体の一実施態様において、前記第１シードは、ユーザデータ領域に非暗号化データとして格納され、前記第２シードは、ユーザデータ領域に暗号化データとして格納された構成であることを特徴とする。

【００３０】

さらに、本発明の情報記録媒体の一実施態様において、前記暗号化データは、トランスポートストリームパケットから構成され、前記第１シードは、複数のトランスポートストリームパケットに対応する制御情報内に格納され、前記第２シードは、前記制御情報外のユーザデータ領域のトランスポートストリームパケット内に暗号化されて格納された構成であることを特徴とする。

【００３１】

さらに、本発明の情報記録媒体の一実施態様において、前記暗号化データは、トランスポートストリームパケットから構成され、前記第１シードは、ユーザデータ領域のトランスポートストリームパケット内に非暗号化データとして格納され、前記第２シードは、ユーザデータ領域のトランスポートストリームパケット

内に暗号化されて格納された構成であることを特徴とする。

【００３２】

さらに、本発明の第６の側面は、

情報記録媒体に格納された暗号化データの復号処理を実行する情報処理方法であり、

情報記録媒体に格納された暗号化データを構成する暗号化処理単位毎に設定された鍵生成情報としての第１シードに基づいて第１ブロックキーＫｂ１を生成するステップと、

生成した第１ブロックキーＫｂ１に基づいて情報記録媒体に格納された暗号化第２シードの復号処理を実行して第２シードを取得し、取得した第２シードに基づいて第２ブロックキーＫｂ２を生成するステップと、

生成した第２ブロックキーＫｂ２に基づく復号処理により前記情報記録媒体に格納された暗号化データの復号処理を実行するステップと、

を有することを特徴とする情報処理方法にある。

【００３３】

さらに、本発明の情報処理方法の一実施態様において、前記情報処理方法は、さらに、記憶手段から読み出したマスターキー生成情報に基づいて生成したマスターキーと、前記情報記録媒体からの読み出し情報とに基づいて、２つの記録キーＫ１，Ｋ２を生成するステップを有し、生成した第１記録キーＫ１と前記第１シード情報とに基づく暗号処理により前記第１ブロックキーＫｂ１を生成し、生成した第１ブロックキーＫｂ１に基づいて情報記録媒体に格納された暗号化第２シードの復号処理を実行して第２シードを取得し、取得した第２シードと第２記録キーＫ２とに基づく暗号処理により前記第２ブロックキーＫｂ２を生成し、生成した第２ブロックキーＫｂ２に基づく復号処理により前記情報記録媒体に格納された暗号化データの復号処理を実行することを特徴とする。

【００３４】

さらに、本発明の情報処理方法の一実施態様において、前記情報処理方法は、前記マスターキーと、前記情報記録媒体からの読み出し情報であるディスクＩＤ、および前記情報記録媒体に記録された２つのタイトルキーに基づいて第１タイ

トル固有キーおよび第２タイトル固有キーを生成し、さらに、前記第１タイトル固有キーと、前記情報記録媒体からの第１読み出し情報とに基づく暗号処理により前記第１記録キーＫ１を生成し、前記第２タイトル固有キーと、前記情報記録媒体からの第２読み出し情報とに基づく暗号処理により前記第２記録キーＫ２を生成するステップを有することを特徴とする。

【００３５】

さらに、本発明の情報処理方法の一実施態様において、前記情報処理方法は、前記マスターキーと、前記情報記録媒体からの読み出し情報であるディスクＩＤ、および前記情報記録媒体に記録された１つのキーシード情報に基づいて第１タイトル固有キーおよび第２タイトル固有キーを生成し、さらに、前記第１タイトル固有キーと、前記情報記録媒体からの第１読み出し情報とに基づく暗号処理により前記第１記録キーＫ１を生成し、前記第２タイトル固有キーと、前記情報記録媒体からの第２読み出し情報とに基づく暗号処理により前記第２記録キーＫ２を生成するステップを有することを特徴とする。

【００３６】

さらに、本発明の第７の側面は、

情報記録媒体に格納された暗号化データの読み取りおよび外部出力を実行する情報処理方法であり、

情報記録媒体に格納された暗号化データの出力先装置との認証処理を実行しセッションキーＫｓを生成する認証処理ステップと、

情報記録媒体に格納された暗号化データを構成する暗号化処理単位毎に設定された鍵生成情報としての第１シードに基づいて第１ブロックキーＫｂ１を生成するステップと、

生成した第１ブロックキーＫｂ１に基づいて情報記録媒体に格納された暗号化第２シードの復号処理を実行して第２シードを取得し、前記セッションキーＫｓに基づいて前記第２シードを含むデータの暗号化処理を実行し出力用暗号化情報を生成するステップと、

前記セッションキーＫｓに基づいて暗号化された第２シードを含む出力用暗号化情報をインタフェースを介して出力するステップと、

を有することを特徴とする情報処理方法にある。

【００３７】

さらに、本発明の情報処理方法の一実施態様において、前記情報処理方法は、情報記録媒体ドライブ装置の保有するマスターキー生成情報に基づいて生成したマスターキーと、前記情報記録媒体からの読み出し情報とに基づいて、２つの記録キーＫ１，Ｋ２を生成し、生成した第１記録キーＫ１と前記第１シード情報とに基づく暗号処理により前記第１ブロックキーＫｂ１を生成し、生成した第１ブロックキーＫｂ１に基づいて情報記録媒体に格納された暗号化第２シードの復号処理を実行して第２シードを取得し、取得した第２シードと第２記録キーＫ２とを含むデータを前記セッションキーＫｓに基づいて暗号化して出力用暗号化情報を生成し、前記第２シードと第２記録キーＫ２とを含む前記出力用暗号化情報をインタフェースを介して出力することを特徴とする。

【００３８】

さらに、本発明の第８の側面は、

データ入力インタフェースを介して入力する暗号データの復号処理を実行する情報処理方法であり、

前記暗号データの出力装置との認証処理を実行しセッションキーＫｓを生成する認証処理ステップと、

前記データ入力インタフェースを介して入力する暗号化情報を前記セッションキーに基づく復号処理により鍵生成情報としてのシード情報および記録キーを取得し、前記シード情報および記録キーに基づく暗号処理により暗号データの復号キーとしてのブロックキーを生成し、該ブロックキーに基づく暗号データの復号処理を実行する暗号処理ステップと、

を有することを特徴とする情報処理方法にある。

【００３９】

さらに、本発明の第９の側面は、

情報記録媒体に格納された暗号化データの読み取りおよび外部出力を実行する情報処理方法であり、

情報記録媒体に格納された暗号化データの出力先装置との認証処理を実行しセ

ッションキーＫｓを生成する認証処理ステップと、

情報記録媒体に格納された暗号化データを構成する暗号化処理単位毎に設定された鍵生成情報としてのシードに基づいてブロックキーを生成し、生成したブロックキーに基づいて情報記録媒体に格納された暗号化データの復号処理を実行して復号データを取得し、前記セッションキーＫｓに基づいて前記復号データの暗号化処理を実行し出力用暗号化情報を生成する暗号処理ステップと、

前記セッションキーＫｓに基づいて暗号化された出力用暗号化情報をインタフェースを介して出力するステップと、

を有することを特徴とする情報処理方法にある。

【００４０】

さらに、本発明の第１０の側面は、

情報記録媒体に格納された暗号化データの復号処理を実行するコンピュータ・プログラムであり、

情報記録媒体に格納された暗号化データを構成する暗号化処理単位毎に設定された鍵生成情報としての第１シードに基づいて第１ブロックキーＫｂ１を生成するステップと、

生成した第１ブロックキーＫｂ１に基づいて情報記録媒体に格納された暗号化第２シードの復号処理を実行して第２シードを取得し、取得した第２シードに基づいて第２ブロックキーＫｂ２を生成するステップと、

生成した第２ブロックキーＫｂ２に基づく復号処理により前記情報記録媒体に格納された暗号化データの復号処理を実行するステップと、

を有することを特徴とするコンピュータ・プログラムにある。

【００４１】

【作用】

本発明においては、本発明の構成によれば、暗号化コンテンツの復号に適用する鍵（ブロックキーＫｂ２）を生成するために必要となるシード情報（シード２）を他の鍵（ブロックキーＫｂ１）によって暗号化して格納する構成としたので、シード情報（シード２）をディスクから直接読み取ることは不可能であり、従ってシード情報を用いて生成される鍵情報の解析、暗号アルゴリズムの解析の困

難性が高まり、セキュリティレベルの高いコンテンツ保護が実現される。

【００４２】

さらに、本発明の構成によれば、情報記録媒体に格納されたデータの再生処理において、暗号化コンテンツの復号に適用する鍵（ブロックキーＫｂ２）生成用のシード情報（シード２）をデバイス間で転送することが必要となる構成において、ブロックキー生成情報、具体的には、シード情報（シード２）および記録キーＫ２の双方をセッションキーで暗号化して送受信する構成としたので、転送路からのデータ漏洩が発生した場合であっても、シード情報（シード２）および記録キーＫ２を取得することは困難となり、シード情報を用いて生成される鍵情報の解析、暗号アルゴリズムの解析の困難性が高まり、セキュリティレベルの高いコンテンツ保護が実現される。

【００４３】

なお、本発明のコンピュータ・プログラムは、例えば、様々なプログラム・コードを実行可能な汎用コンピュータ・システムに対して、コンピュータ可読な形式で提供する記憶媒体、通信媒体、例えば、ＣＤやＤＶＤ、ＭＯなどの記憶媒体、あるいは、ネットワークなどの通信媒体によって提供可能なコンピュータ・プログラムである。このようなプログラムをコンピュータ可読な形式で提供することにより、コンピュータ・システム上でプログラムに応じた処理が実現される。

【００４４】

本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。なお、本明細書においてシステムとは、複数の装置の論理的集合構成であり、各構成の装置が同一筐体内にあるものには限らない。

【００４５】

【発明の実施の形態】

［記録媒体上のデータ記録構成］

まず、本発明に係る情報記録媒体に格納されたデータ構成について説明する。情報記録媒体に格納された暗号化データは、データ記録再生装置や、ＰＣ（パーソナルコンピュータ）において読み取られ、復号、再生される。

【００４６】

情報記録媒体に格納されるデータは、例えばＭＰＥＧ－２システムで規定されている符号化データとしてのトランスポートストリーム（ＴＳ）である。トランスポートストリームは、１本のストリームの中に複数のプログラムを構成することができ、各トランスポートパケットの出現タイミング情報としてのＡＴＳ（Arrival Time Stamp：着信時刻スタンプ）が設定されている。このタイムスタンプは、ＭＰＥＧ－２システムで規定されている仮想的なデコーダであるＴ－ＳＴＤ(Transport stream System Target Decoder)を破綻させないように符号化時に決定され、ストリームの再生時に、各トランスポートパケットに付加されたＡＴＳによって出現タイミングを制御して、復号、再生を行う。

【００４７】

例えば、トランスポートストリームパケットを記録媒体に記録する場合には、各パケットの間隔を詰めたソースパケットとして記録するが、各トランスポートパケットの出現タイミングを併せて記録媒体に保存することにより、再生時に各パケットの出力タイミングを制御することが可能となる。

【００４８】

図１を参照して、情報記録媒体に格納されるデータ記録構成および、記録データの復号再生処理の概要を説明する。情報記録媒体に格納されるデータは暗号化データであり、再生を行う場合には、復号処理を行うことが必要となる。図１（ａ）が情報記録媒体に格納されるデータ記録構成である。１８バイトの制御データ（User Control Data）と、２０４８バイトのユーザデータ(User Data)が１つのセクタデータとして構成され、例えば３セクタ分のデータが１つの暗号処理単位として規定される。なおここで説明するバイト数や、処理単位は１つの代表例であり、制御データ、ユーザデータのバイト数や、処理単位の設定は、様々な設定が可能である。

【００４９】

（ｂ）は、暗号処理単位である１ユニット（１ＡＵ：Aligned Unit）の構成を示す。情報記録媒体に格納された暗号化データの再生を実行する情報処理装置は、制御データ内のフラグに基づいて、暗号処理単位である１ＡＵ（Aligned Unit

）を抽出する。

【００５０】

暗号処理単位である１ユニット（１ＡＵ）には、（ｃ）暗号化構成に示すように、ブロックキーＫｂ１によって暗号化された領域、ブロックキーＫｂ２によって暗号化された領域が含まれる。ブロックキーＫｂ１とＫｂ２によって二重に暗号化された領域を含める構成としてもよい。ブロックキーを生成するためには、鍵生成情報としてのシード情報が必要となる。シード情報（シード１）はブロックキーＫｂ１を生成するための鍵生成情報であり、シード情報（シード２）はブロックキーＫｂ２を生成するための鍵生成情報である。これらは、制御データ領域、あるいはユーザデータ領域に格納される。図１（ｃ）に示すシード情報の格納態様、暗号化態様は一例であり、後段において、複数の構成例について説明する。

【００５１】

ユーザデータ領域に格納された暗号化コンテンツを復号するためには、情報記録媒体に格納されたシード情報を読み取って、シード情報に基づく鍵を生成することが必要となる。

【００５２】

本発明の構成においては、図１（ｃ）に示すように、ブロックキーＫｂ１を生成するために必要となるシード情報（シード１）と、ブロックキーＫｂ２を生成するために必要となるシード情報（シード２）とを情報記録媒体上に格納する構成とするとともに、一方のシード情報（シード２）をシード情報（シード１）によって生成されるブロックキーＫｂ１によって暗号化して格納する構成とした。

【００５３】

このように、本発明の構成は、２つの異なる鍵を適用した暗号化処理を実行したデータを記録媒体に格納し、再生処理において２つの異なる鍵を適用した復号処理を行う。すなわち、所定の暗号処理単位毎に異なる鍵生成情報であるシード１、シード２を適用した暗号処理によりブロックキーＫｂ１，Ｋｂ２を生成して復号処理を実行する。

【００５４】

１処理単位毎の復号処理の後、復号されたトランスポートストリームパケットがＭＰＥＧ－２デコーダに入力されデコード処理が実行されてコンテンツ再生が行なわれる。１つの処理単位（３セクタ）には、例えば３２個のトランスポートストリーム（ＴＳ）パケットが含まれる。すなわち、３２×１９２＝６１４４バイトデータが１つの暗号化および復号処理単位とされる。なお、処理単位の設定は、様々な設定が可能である。

【００５５】

復号再生時には、各処理単位毎に２つのシード情報（シード１、シード２）を情報記録媒体から取得し、各シード情報に基づいて２つのブロックキーＫｂ１、Ｋｂ２を生成し、生成したブロックキーＫｂ１，Ｋｂ２を用いて復号処理がなされて、コンテンツ再生が行われる。

【００５６】

また、コンテンツの記録時には、復号再生処理と逆のプロセスが実行され、各処理単位毎に２つのシード情報（シード１、シード２）を設定し、各シード情報に基づいて２つのブロックキーＫｂ１、Ｋｂ２を生成し生成したブロックキーＫｂ１，Ｋｂ２を用いて暗号化処理がなされて、コンテンツ記録が行われる。

【００５７】

[情報処理装置構成]

図２は、上述した暗号化コンテンツ態様を持つコンテンツの記録再生処理を実行する情報処理装置１００の一実施例構成を示すブロック図である。情報処理装置１００は、入出力Ｉ／Ｆ(Interface)１２０、ＭＰＥＧ(Moving Picture Experts Group)コーデック１３０、Ａ／Ｄ，Ｄ／Ａコンバータ１４１を備えた入出力Ｉ／Ｆ(Interface)１４０、暗号処理手段１５０、ＲＯＭ (Read Only Memory)１６０、ＣＰＵ(Central Processing Unit)１７０、メモリ１８０、記録媒体１９５のドライブ１９０、さらにトランスポートストリーム処理手段（ＴＳ処理手段）１９８を有し、これらはバス１１０によって相互に接続されている。

【００５８】

入出力Ｉ／Ｆ１２０は、外部から供給される画像、音声、プログラム等の各種コンテンツを構成するデジタル信号を受信し、バス１１０上に出力するとともに

、バス１１０上のデジタル信号を受信し、外部に出力する。ＭＰＥＧコーデック１３０は、バス１１０を介して供給されるＭＰＥＧ符号化されたデータを、ＭＰＥＧデコードし、入出力Ｉ／Ｆ１４０に出力するとともに、入出力Ｉ／Ｆ１４０から供給されるデジタル信号をＭＰＥＧエンコードしてバス１１０上に出力する。入出力Ｉ／Ｆ１４０は、Ａ／Ｄ，Ｄ／Ａコンバータ１４１を内蔵している。入出力Ｉ／Ｆ１４０は、外部から供給されるコンテンツとしてのアナログ信号を受信し、Ａ／Ｄ，Ｄ／Ａコンバータ１４１でＡ／Ｄ(Analog Digital)変換することで、デジタル信号として、ＭＰＥＧコーデック１３０に出力するとともに、ＭＰＥＧコーデック１３０からのデジタル信号を、Ａ／Ｄ，Ｄ／Ａコンバータ１４１でＤ／Ａ(Digital Analog)変換することで、アナログ信号として、外部に出力する。

【００５９】

暗号処理手段１５０は、例えば、１チップのＬＳＩ(Large Scale Integrated Circuit)で構成され、バス１１０を介して供給されるコンテンツとしてのデジタル信号を暗号化し、または復号し、バス１１０上に出力する構成を持つ。なお、暗号処理手段１５０は１チップＬＳＩに限らず、各種のソフトウェアまたはハードウェアを組み合わせた構成によって実現することも可能である。暗号処理手段１５０は、さらに、例えば入出力Ｉ／Ｆ１２０を介して接続された外部装置とのコンテンツ入出力の際に実行する認証処理を実行する認証処理部としても機能する。

【００６０】

ＲＯＭ１６０は、例えば、情報処理装置ごとに固有の、あるいは、複数の情報処理装置のグループごとに固有のデバイスキーや、相互認証時に必要とする認証キーを記憶している。デバイスキーは、例えば鍵配信ツリー構成に基づいて提供される暗号化鍵ブロック情報としてのＥＫＢ（Enabling Key Block）を復号してマスターキーを取得するために用いられる。すなわち、デバイスキーは、マスターキー生成情報として適用される。

【００６１】

ＣＰＵ１７０は、メモリ１８０に記憶されたプログラムを実行することで、Ｍ

ＰＥＧコーデック１３０や暗号処理手段１５０等を制御する。メモリ１８０は、例えば、不揮発性メモリで、ＣＰＵ１７０が実行するプログラムや、ＣＰＵ１７０の動作上必要なデータを記憶する。ドライブ１９０は、デジタルデータを記録再生可能な記録媒体１９５を駆動することにより、記録媒体１９５からデジタルデータを読み出し（再生し）、バス１１０上に出力するとともに、バス１１０を介して供給されるデジタルデータを、記録媒体１９５に供給して記録させる。なお、プログラムをＲＯＭ１６０に、マスターキー生成情報や認証キーをメモリ１８０に記憶するように構成してもよい。

【００６２】

記録媒体１９５は、例えば、ＤＶＤ、ＣＤ等の光ディスク、光磁気ディスク、磁気ディスク、磁気テープ、あるいはフラッシュＲＯＭ、ＭＲＡＭ、ＲＡＭ等の半導体メモリ等のデジタルデータの記憶可能な媒体であり、本実施の形態では、ドライブ１９０に対して着脱可能な構成であるとする。但し、記録媒体１９５は、情報処理装置１００に内蔵する構成としてもよい。

【００６３】

トランスポートストリーム処理手段（ＴＳ処理手段）１９８は、複数のコンテンツが多重化されたトランスポートストリームから特定のコンテンツに対応するトランスポートパケットを取り出して、取り出したトランスポートストリームの出現タイミング情報を各パケットとともに記録媒体１９５に格納するためのデータ処理を実行し、また、記録媒体１９５からの暗号化コンテンツの復号再生時には、トランスポートストリームの出現タイミング制御を行なう。

【００６４】

トランスポートストリームには、前述したように、各トランスポートパケットの出現タイミング情報としてのＡＴＳ（Arrival Time Stamp：着信時刻スタンプ）が設定されており、ＭＰＥＧ２デコーダによる復号時にＡＴＳによってタイミング制御を実行する。トランスポートストリーム処理手段（ＴＳ処理手段）１９８は、例えば、トランスポートパケットを記録媒体に記録する場合には、各パケットの間隔を詰めたソースパケットとして記録するが、各トランスポートパケットの出現タイミングを併せて記録媒体に保存することにより、再生時に各パケッ

トの出力タイミングを制御することが可能となる。

【００６５】

本発明の情報処理装置１００は、例えば上述のトランスポートストリームによって構成される暗号化コンテンツの記録再生を実行する。これらの処理の詳細については、後段で説明する。なお、図２に示す暗号処理手段１５０、ＴＳ処理手段１９８は、理解を容易にするため、別ブロックとして示してあるが、両機能を実行する１つのワンチップＬＳＩとして構成してもよく、また、両機能をソフトウェアまたはハードウェアを組み合わせた構成によって実現する構成としてもよい。さらには、ドライブ１９０、記録媒体１９５を除く全てのブロックをワンチップＬＳＩとして構成してもよく、また、これらの機能をソフトウェアまたはハードウェアを組み合わせた構成によって実現する構成としてもよく、これにより情報処理装置１００の改造によるセキュリティ機能の無効化に対するロバストネスを向上させることが出来る。

【００６６】

［データ再生処理］

次に、記録媒体に格納された暗号化データの復号処理について説明する。図３にデータの復号処理の手順を説明する図を示す。図３に示す処理は、主に図２に示す暗号処理手段１５０が実行する処理である。

【００６７】

情報処理装置２１０は自身のメモリ１８０（図２参照）に格納しているマスターキー２１１を読み出す。マスターキー２１１は、ライセンスを受けた情報処理装置に格納された秘密キーであり、複数の情報処理装置に共通なキーとして格納された共通キーである。情報処理装置２１０は情報記録媒体２２０に識別情報としてのディスクＩＤ（Disc ID）２２１が既に記録されているかどうかを検査する。記録されていれば、ディスクＩＤ（Disc ID）２２１を情報記録媒体２２０から読出す。ディスクＩＤ（Disc ID）２２１は、ディスク固有情報であり、例えば一般データ格納領域または、リードインエリアに格納される。

【００６８】

次に、情報処理装置２１０は、ステップＳ１０１において、マスターキー２１

１とディスクＩＤ２２１を用いて、ディスク固有キー（Disc Unique Key）を生成する。ディスク固有キー（Disc Unique Key）の具体的な生成方法としては、例えば、図４（ａ）に示すように、ディスクＩＤ（Disc ID）を入力値とし、共通鍵暗号方式であるＡＥＳ（Advanced Encryption Standard）暗号を、マスターキー（Master Key）を暗号鍵として実行する方法や、図４（ｂ）に示すように、FIPS 180-1で定められているハッシュ関数ＳＨＡ－１に、マスターキーとディスクＩＤ（Disc ID）とのビット連結により生成されるデータを入力し、その出力から必要なデータ長のみをディスク固有キー（Disc Unique Key）として使用する方法が適用できる。

【００６９】

次に、記録コンテンツごとの２つの固有鍵であるタイトルキー（Title Key）１，２２３、タイトルキー２，２２４を情報記録媒体２２０から読出す。ディスク上には、どこのデータがどんなタイトルを構成するかという情報が格納されたデータ管理ファイルがあり、このファイルにタイトルキーが格納されている。ディスク１枚に対してタイトルキーが１組しかない場合、すなわちディスクＩＤ２２１に対するタイトルキーが一意に決定できる場合には、ディスクＩＤ２２１と同様の方法で、例えば一般データ格納領域または、リードインエリアに格納するようにしてもよい。

【００７０】

次にステップＳ１０２およびステップＳ１０３において、ディスク固有キー（Disc Unique Key）とタイトルキー（Title Key）１，２から、２つのタイトル固有キー（Title Unique Key）１，２を生成する。この生成の具体的な方法も、上記のように、SHA-1を用いる方法やブロック暗号に基づくハッシュ関数を使用する方法などが適用可能である。

【００７１】

さらに、情報処理装置２１０は、ステップＳ１０２およびステップＳ１０３において生成した２つのタイトル固有キー（Title Unique Key）１，２と、情報記録媒体２２０から読み出した記録シード（ＲＥＣ　ＳＥＥＤ）２２５、物理インデックス２２６とに基づいて、ステップＳ１０４、Ｓ１０５において、２つの記

録キー（ＲＥＣキー）Ｋ１，Ｋ２を生成する。

【００７２】

ステップＳ１０２～Ｓ１０５において実行する２つの記録キー（ＲＥＣキー）Ｋ１，Ｋ２の生成処理例について、図５を参照して説明する。

【００７３】

図５（ａ）は、図３のステップＳ１０２，Ｓ１０４の処理による記録キーＫ１の生成、図５（ｂ）は、図３のステップＳ１０３，Ｓ１０５の処理による記録キーＫ２の生成処理例を示している。

【００７４】

図５（ａ）の処理は、まず情報記録媒体から読み出したタイトルキー１をＡＥＳ（Advanced Encryption Standard）暗号処理部２７１に入力し、ステップＳ１０１で生成したディスク固有キーを適用した復号処理（Decryption）を実行してタイトル固有キー１を生成（Ｓ１０２）して、さらに、情報記録媒体から読み出した物理インデックス２２６をＡＥＳ（Advanced Encryption Standard）暗号処理部２７２に入力し、タイトル固有キー１を適用した暗号処理（Encryption）を実行し、さらに、排他論理和部２７３において、暗号処理結果とタイトル固有キー１の排他論理和演算を実行して、その出力を記録キー１として設定（Ｓ１０４）する処理である。

【００７５】

図５（ｂ）の処理は、情報記録媒体から読み出したタイトルキー２をＡＥＳ（Advanced Encryption Standard）暗号処理部２７４に入力し、ステップＳ１０１で生成したディスク固有キーを適用した復号処理（Decryption）を実行してタイトル固有キー２を生成（Ｓ１０３）して、さらに、情報記録媒体から読み出した記録シード（ＲＥＣ　ＳＥＥＤ）２２５をＡＥＳ（Advanced Encryption Standard）暗号処理部２７５に入力し、タイトル固有キー２を適用した暗号処理（Encryption）を実行して記録キー２を生成（Ｓ１０５）する処理である。

【００７６】

記録キーＫ１、Ｋ２は、上述の再生処理プロセスにおいて使用することが必要となるが、コンテンツを情報記録媒体に記録する暗号処理においても適用される

鍵である。

【００７７】

図６に示すように、情報記録媒体２８４に格納される暗号化コンテンツは、まずコンテンツ編集スタジオ２８２において編集され、編集コンテンツがディスク製造工場等のディスク製造エンティテイ２８３に渡されて、ディスク等の情報記録媒体に格納され、ユーザに提供される。

【００７８】

この製造プロセスにおいて、コンテンツ編集スタジオ２８２は、物理インデックスを設定するとともに、記録キーＫ２を適用した暗号化処理を編集コンテンツに対して実行し、ディスク製造エンティテイ２８３は、記録シードを設定するとともに、記録キーＫ１を適用した暗号化処理を実行する。結果として情報記録媒体２８４には、記録キーＫ１、Ｋ２の２つの暗号鍵を用いた暗号処理が施された暗号化データが格納される。このようなディスク製造プロセスにおいて、コンテンツの管理を実行する管理センタ２８１が、コンテンツ編集スタジオには、タイトル固有キー２の取得可能情報を提供し、ディスク製造エンティテイ２８３には、タイトル固有キー１の取得可能情報を提供する。

【００７９】

管理センタ２８１がこのような鍵管理を実行することで、管理センタ２８１からの鍵情報の提供を受けたコンテンツ編集スタジオ、およびディスク製造エンティテイのみが、暗号化コンテンツの格納された情報記録媒体の製造が可能となり、不正な第三者による海賊版ディスクの製造が防止される。特に、コンテンツ編集スタジオが編集コンテンツに適用されるＴＳパケット内に編集識別子（編集ＩＤ）を格納して、これを編集コンテンツとともにコンテンツ編集スタジオで暗号化処理を施すことで、どの編集スタジオで加工された編集コンテンツであるかを秘匿したままディスク製造エンティテイへデータを渡すことが可能となり、ディスク製造エンティテイが受け入れるコンテンツの追跡管理が可能となる。

【００８０】

なお、図３に示す例では、２つのタイトル固有キー１，２を算出するために、情報記録媒体２２０に２つのタイトルキー１，２を格納し、これらの２つのタイ

トルキーに基づいて、２つのタイトル固有キーを算出する処理例を示したが、このように２つのタイトルキーを情報記録媒体２２０に格納することなく、１つの格納情報のみから、２つのタイトル固有キー１，２を算出する構成も可能である。

【００８１】

図７を参照して１つの格納情報のみから、２つのタイトル固有キー１，２を算出する構成例を説明する。編集（オーサリング）毎に設定される乱数等のランダム値をディスクキーシードとして情報記録媒体２２０に格納する。

【００８２】

図７（ａ）の処理例は、ディスクキーシードに対してディスク固有キーを適用して、ＡＥＳ暗号処理部２９１において暗号処理を実行し、その出力をタイトル固有キー１とする。さらにそのタイトル固有キー１をＡＥＳ暗号処理部２９２に入力しディスク固有キーを適用してＡＥＳ暗号処理を実行し、その結果をタイトル固有キー２とする。

【００８３】

図７（ｂ）の処理例は、ディスクキーシードに対してディスク固有キーを適用して、ＡＥＳ暗号処理部２９３において暗号処理を実行し、その出力をタイトル固有キー１とする。さらにそのタイトル固有キー１を、演算部２９４において、演算、例えば、（ディスクキーシード＋１）ｍｏｄ２128を算出し、その結果をＡＥＳ暗号処理部２９５に入力しディスク固有キーを適用してＡＥＳ暗号処理を実行し、その結果をタイトル固有キー２とする。図７に示す方法によれば、情報記録媒体２２０に格納する情報を少なくすることが可能となる。

【００８４】

図３に戻り、情報記録媒体からのデータ復号、再生処理についての説明を続ける。ステップＳ１０４、Ｓ１０５において２つの記録キー（ＲＥＣキー）１，２を生成すると、次に、ステップＳ１０６において、ブロックキーＫｂ１の生成処理を実行する。

【００８５】

ブロックキーＫｂ１の生成処理においては、情報記録媒体２２０からブロック

キーＫｂ１生成情報としてのシード情報（シード１）２２７を読み出し、シード情報（シード１）２２７と、ステップＳ１０４において生成した記録キーＫ１とに基づく暗号処理を実行してブロックキーＫｂ１を生成する。

【００８６】

ステップＳ１０６のブロックキーＫｂ１の生成処理以降に実行する処理について、図８を参照して説明する。

【００８７】

図８において、復号処理は、処理単位３００を単位として実行される。この処理単位は、先に図１を参照して説明した（ｂ）処理単位に相当する。すなわち、暗号処理単位である１ユニット（１ＡＵ：Aligned Unit）である。情報記録媒体２２０に格納された暗号化データの再生を実行する情報処理装置２１０は、制御データ内のフラグに基づいて、暗号処理単位である１ＡＵ（Aligned Unit）を抽出する。

【００８８】

処理単位３００には、１８バイトの制御データ３０１と、６１４４バイトのユーザデータ（暗号化コンテンツを含む）が含まれる。６１４４バイトのユーザデータは、トランスポートストリームパケットの単位である１９２バイト毎に分割される。ユーザデータの先頭のＴＳパケット３０２と、後続の５９５２バイトのＴＳパケット群３０３を分離して説明する。この例では、シード情報（シード１）３１１が制御データ３０１に格納され、シード情報（シード２）３１２がユーザデータ内の先頭のＴＳパケット３０２内に暗号化されて格納された例である。

【００８９】

なお、シード情報としての、シード１、シード２の格納態様には複数の態様があり、ここではその一例を示す。他の例については、後段で説明する。

【００９０】

図８において、図３の処理ステップと同様の処理ステップには、同一の処理ステップ番号を付してある。

【００９１】

ステップＳ１０６（図３、図８）においては、情報記録媒体の制御データ内か

ら読み出したシード情報（シード1）３１１をＡＥＳ暗号処理部に入力し、先のステップＳ１０４において生成した記録キーＫ１を適用したＡＥＳ暗号処理を実行しブロックキーＫｂ１を生成する処理を実行する。なお、図８においてＡＥＳ＿Ｇは、ＡＥＳ暗号処理を適用した鍵生成（Key Generation）処理を示し、ＡＥＳ＿Ｄは、ＡＥＳ暗号処理を適用したデータ復号（Decryption）処理を示している。

【００９２】

次に、図３のステップＳ１０７において、３２ＴＳパケットからなるユーザデータから暗号化データ部のみが抽出される。ユーザデータの暗号化部、非暗号化部がステップＳ１０７において分離されて、暗号化部のみがステップＳ１０８～Ｓ１１１の復号処理プロセス対象とされる。非暗号化部は、ステップＳ１０８～Ｓ１１１をスキップし、ステップＳ１１２において、再度セレクタステップにより復号データと連結され、復号ＴＳパケット群として、例えばＭＰＥＧデコーダに入力され、デコード処理がなされる。

【００９３】

ステップＳ１０８（図３、図８参照）では、ステップＳ１０６において生成したブロックキーＫｂ１を適用したＡＥＳ復号処理を実行する。ステップＳ１０８では、ブロックキーＫｂ１を適用した暗号処理のなされたデータ部のみを対象とした復号処理が実行される。この例では、ユーザデータの先頭ＴＳパケット３０２の少なくともシード情報（シード2）を含むデータ領域がブロックキーＫｂ１を適用した暗号処理のなされたデータ部である。従って、このシード情報（シード2）を含むデータ領域を対象としてブロックキーＫｂ１を適用した復号処理を実行する。

【００９４】

なお、ブロックキーＫｂ１を適用した暗号処理のなされたデータ部をどのデータ領域とするかについては、いくつかのパターンがあり、これらについては後述する。

【００９５】

先頭ＴＳパケット３０２には、他のユーザデータ部、すなわち、後続の５９５

２バイトのＴＳパケット群３０３の復号処理に適用するブロックキーＫｂ２を算出するために必要となるシード情報（シード２）３１２が含まれている。すなわち、シード情報（シード２）３１２は、ブロックキーＫｂ１を適用した暗号処理がなされた暗号化データとして先頭ＴＳパケット３０２に記録されている。

【００９６】

ステップＳ１０６における、ブロックキーＫｂ１を適用した復号処理の結果として、復号ＴＳパケット３０４が算出され、その中からシード情報（シード２）を抽出する。

【００９７】

図３のセレクタステップＳ１０９は、ブロックキーＫｂ１を適用した復号処理の結果から、シード情報（シード２）をステップＳ１１０のブロックキーＫｂ２生成ステップに出力し、ブロックキーＫｂ２で暗号化された暗号化データを復号ステップＳ１１１に出力し、その他の復号データ（非暗号化データ）をセレクタステップＳ１１２に出力することを示している。

【００９８】

ステップＳ１１０（図３，図８参照）では、ステップＳ１０８におけるブロックキーＫｂ１を適用した復号処理の結果取得された復号ＴＳパケット３０４から抽出したシード情報（シード２）と、ステップＳ１０５（図３参照）において生成した記録キーＫ２とに基づいて、ＡＥＳ暗号処理を実行し、ブロックキーＫｂ２を算出する。

【００９９】

次に、ステップＳ１１１において、ブロックキーＫｂ２を適用してユーザデータ部の暗号化部（ブロックキーＫｂ２で暗号化されたデータ領域３０３）を復号し、復号ＴＳパケット群３０５を生成する。

【０１００】

復号ＴＳパケット群３０５、および復号ＴＳパケット３０４は、セレクタステップＳ１１２において結合されて、復号ＴＳパケットとして例えばＭＰＥＧ２デコーダに入力され、デコードされた後、再生される。

【０１０１】

このように、本発明の構成においては、暗号化コンテンツの復号に適用する鍵（ブロックキーＫｂ２）を生成するために必要となるシード情報（シード２）を他の鍵（ブロックキーＫｂ１）によって暗号化して格納する構成としたので、シード情報（シード２）をディスクから直接読み取ることは不可能であり、従ってシード情報を用いて生成される鍵情報の解析、暗号アルゴリズムの解析の困難性が高まり、セキュリティレベルの高いコンテンツ保護が実現される。

【０１０２】

なお、２つのシード情報の格納形態には、様々な態様があり、以下、複数の例について説明する。

【０１０３】

図９に、シード情報（シード１）と、シード情報（シード２）とを共にユーザデータ内の先頭ＴＳパケット３０２内に格納した例を示す。先に図８を参照して説明した例では、シード情報（シード１）３１１が制御データ３０１に格納され、シード情報（シード２）３１２がユーザデータ内の先頭のＴＳパケット３０２内に暗号化されて格納された例を説明したが、図９に示す構成例は、シード情報（シード１）３２１、シード情報（シード２）３２２、双方がユーザデータ内の先頭のＴＳパケット３０２内に格納された例である。

【０１０４】

なお、シード情報（シード２）３２２は、図８において説明した例と同様、シード情報（シード１）３２１を適用して取得されるブロックキーＫｂ１によって暗号化されてユーザデータ内の先頭のＴＳパケット３０２内に格納される。

【０１０５】

図９において、復号処理は、処理単位３００を単位として実行される。この処理単位は、先に図１を参照して説明した（ｂ）処理単位に相当する１ユニット（１ＡＵ：Aligned Unit）である。情報記録媒体２２０に格納された暗号化データの再生を実行する情報処理装置２１０は、制御データ内のフラグに基づいて、暗号処理単位である１ＡＵ（Aligned Unit）を抽出する。

【０１０６】

あるいは、暗号化処理単位ごとに暗号化が施されたユニットであるか暗号化が

施されていないユニットであるかを判別するため、暗号化処理単位の先頭に存在するシード情報３２１に含まれるフラグを利用する構成とすることができる。シード情報を含めた暗号化処理単位の先頭部分を表した例が図１０である。図１０のコピー制御情報としてのＣＣＩ部分に記録されたフラグを利用して暗号化の有無を判別することができる。暗号化されている場合は復号化を行う経路を通し再生を行う。暗号化されていない場合は復号化を行う経路を通さずに再生を行う。

【０１０７】

図１１に、ＣＣＩ部分に記録されたフラグを利用して暗号化の有無を判別し、暗号化されている場合は復号化を行う経路を通し再生を行い、暗号化されていない場合は復号化を行う経路を通さずに再生を行う処理を実行する場合の処理構成を示す。図１１において、先の図３に示す構成との違いは、セレクタステップＳ１０７が、シード情報（シード１）２２７を入力し、シード情報（シード１）２２７のＣＣＩ部分に記録されたフラグを利用して暗号化の有無を判別し、暗号化されている場合は復号化を行う経路を通し、暗号化されていない場合は復号化を行う経路を通さずに再生を行う選択処理を実行する点のみである。他の処理は、図３に示す処理と同様である。

【０１０８】

図９の処理について説明する。図９において、図３または図１１の処理ステップと同様の処理ステップには、同一の処理ステップ番号を付してある。

【０１０９】

ステップＳ１０６（図１１、図９）は、情報記録媒体のユーザデータの先頭ＴＳパケット内から読み出したシード情報（シード１）３２１をＡＥＳ暗号処理部に入力し、先のステップＳ１０４（図１１参照）において生成した記録キーＫ１を適用したＡＥＳ暗号処理を実行しブロックキーＫｂ１生成処理を実行するステップである。

【０１１０】

次に、図１１のステップＳ１０７において、３２ＴＳパケットからなるユーザデータから暗号化データ部のみが抽出される。ユーザデータの暗号化部、非暗号化部がステップＳ１０７において分離されて、暗号化部のみがステップＳ１０８

～Ｓ１１１の復号処理プロセス対象とされる。非暗号化部は、ステップＳ１０８～Ｓ１１１をスキップし、ステップＳ１１２において、再度セレクタステップにより復号データと連結され、復号ＴＳパケット群として、例えばＭＰＥＧデコーダに入力され、デコード処理がなされる。

【０１１１】

ステップＳ１０８（図１１、図９参照）では、ステップＳ１０６において生成したブロックキーＫｂ１を適用したＡＥＳ復号処理が実行される。ステップＳ１０８では、ブロックキーＫｂ１を適用した暗号処理のなされたデータ部のみを対象とした復号処理が実行される。この例では、ユーザデータの先頭ＴＳパケット３０２中、少なくともシード情報（シード２）３２２を含むデータ領域の復号処理が実行される。

【０１１２】

この先頭ＴＳパケット３０２の暗号化データ領域には、他のユーザデータ部、すなわち、後続の５９５２バイトのＴＳパケット群３０３の復号処理に適用するブロックキーＫｂ２を算出するために必要となるシード情報（シード２）３２２が含まれている。すなわち、シード情報（シード２）３２２は、ブロックキーＫｂ１を適用した暗号処理がなされた暗号化データとして先頭ＴＳパケット３０２に記録されている。

【０１１３】

ステップＳ１０６における、ブロックキーＫｂ１を適用した復号処理の結果として、復号ＴＳパケット３０４が算出され、その中からシード情報（シード２）を抽出する。

【０１１４】

図３のセレクタステップＳ１０９は、ブロックキーＫｂ１を適用した復号処理の結果から、シード情報（シード２）をステップＳ１１０のブロックキーＫｂ２生成ステップに出力し、ブロックキーＫｂ２で暗号化された暗号化データを復号ステップＳ１１１に出力し、その他の復号データ（非暗号化データ）をセレクタステップＳ１１２に出力することを示している。

【０１１５】

ステップＳ１１０（図１１，図９参照）では、ステップＳ１０８におけるブロックキーＫｂ１を適用した復号処理の結果取得された復号ＴＳパケット３０４から抽出したシード情報（シード２）と、ステップＳ１０５（図１１参照）において生成した記録キーＫ２とに基づいて、ＡＥＳ暗号処理を実行し、ブロックキーＫｂ２を算出する。

【０１１６】

次に、ステップＳ１１１において、ブロックキーＫｂ２を適用してユーザデータ部の暗号化部（ブロックキーＫｂ２で暗号化されたデータ領域３０３）を復号し、復号ＴＳパケット群３０５を生成する。

【０１１７】

復号ＴＳパケット群３０５、および復号ＴＳパケット３０４は、セレクタステップＳ１１２において結合されて、復号ＴＳパケットとして例えばＭＰＥＧ２デコーダに入力され、デコードされた後、再生される。

【０１１８】

このように、本構成においては、シード情報（シード１）と、シード情報（シード２）とを共にユーザデータ内の先頭ＴＳパケット内に格納し、ブロックキーＫｂ２を生成するために必要となるシード情報（シード２）は、シード情報（シード１）と、記録キーＫ１とに基づいて生成するブロックキーＫｂ１によって暗号化して格納する構成とした。

【０１１９】

本構成においても、シード情報（シード２）をディスクから直接読み取ることは不可能であり、従ってシード情報を用いて生成される鍵情報の解析、暗号アルゴリズムの解析の困難性が高まり、セキュリティレベルの高いコンテンツ保護が実現される。

【０１２０】

図１２に示す例は、シード情報（シード１）３３１をユーザデータ内の先頭ＴＳパケット３０２に格納し、シード情報（シード２）３３２をユーザデータ内の次のＴＳパケット３４１に格納した例である。

【０１２１】

なお、シード情報（シード２）３３２は、図８、図９において説明した例と同様、シード情報（シード１）３３１を適用して取得されるブロックキーＫｂ１によって暗号化されてユーザデータ内の第２のＴＳパケット３４１内に格納される。

【０１２２】

図１２において、復号処理は、処理単位３００を単位として実行される。この処理単位は、先に図１を参照して説明した（ｂ）処理単位に相当する１ユニット（１ＡＵ：Aligned Unit）である。情報記録媒体２２０に格納された暗号化データの再生を実行する情報処理装置２１０は、制御データ内のフラグに基づいて、暗号処理単位である１ＡＵ（Aligned Unit）を抽出する。

【０１２３】

あるいは、暗号化処理単位ごとに暗号化が施されたユニットであるか暗号化が施されていないユニットであるかを判別するため、暗号化処理単位の先頭に存在するシード情報３２１に含まれるフラグを利用する。シード情報を含めた暗号化処理単位の先頭部分を表した例が図１０である。図１０のＣＣＩ部分に記録されたフラグを利用して暗号化の有無を判別することができる。暗号化されている場合は復号化を行う経路を通し再生を行う。暗号化されていない場合は復号化を行う経路を通さずに再生を行う。

【０１２４】

図１２の処理について説明する。図１２において、図３または図１１の処理ステップと同様の処理ステップには、同一の処理ステップ番号を付してある。

【０１２５】

ステップＳ１０６（図１１、図１２）は、情報記録媒体のユーザデータの先頭ＴＳパケット内から読み出したシード情報（シード１）３３１をＡＥＳ暗号処理部に入力し、先のステップＳ１０４（図１１参照）において生成した記録キーＫ１を適用したＡＥＳ暗号処理を実行してブロックキーＫｂ１を生成するステップである。

【０１２６】

次に、図３のステップＳ１０７において、３２ＴＳパケットからなるユーザデ

ータから暗号化データ部のみが抽出される。ユーザデータの暗号化部、非暗号化部がステップＳ１０７において分離されて、暗号化部のみがステップＳ１０８～Ｓ１１１の復号処理プロセス対象とされる。非暗号化部は、ステップＳ１０８～Ｓ１１１をスキップし、ステップＳ１１２において、再度セレクタステップにより復号データと連結され、復号ＴＳパケット群として、例えばＭＰＥＧデコーダに入力され、デコード処理がなされる。

【０１２７】

ステップＳ１０８（図１１、図１２参照）では、ステップＳ１０６において生成したブロックキーＫｂ１を適用したＡＥＳ復号処理を実行する。復号処理対象は、ブロックキーＫｂ１を適用した暗号処理がなされているデータ領域であり、ユーザデータの先頭ＴＳパケット中のシード情報（シード１）３２１を除くデータ領域の暗号化領域と、第２ＴＳパケット中の少なくともシード情報（シード２）３３２を含むデータ領域の復号処理が実行される。ブロックキーＫｂ１を適用した暗号処理のなされたデータ部をどのデータ領域とするかについては、いくつかのパターンがあり、これらについては後述する。

【０１２８】

本例では、第２のＴＳパケット３４１の暗号化データ領域に、他のユーザデータ部、すなわち、後続のＴＳパケット群３４２の復号処理に適用するブロックキーＫｂ２を算出するために必要となるシード情報（シード２）３３２が含まれる。すなわち、シード情報（シード２）３３２は、ブロックキーＫｂ１を適用した暗号処理がなされた暗号化データとして第２ＴＳパケット３４１に記録されている。

【０１２９】

ステップＳ１０６における、ブロックキーＫｂ１を適用した復号処理の結果として、復号ＴＳパケット３０４が算出され、その中からシード情報（シード２）を抽出する。

【０１３０】

図１１のセレクタステップＳ１０９は、ブロックキーＫｂ１を適用した復号処理の結果から、シード情報（シード２）をステップＳ１１０のブロックキーＫｂ

２生成ステップに出力し、ブロックキーＫｂ２で暗号化された暗号化データを復号ステップＳ１１１に出力し、その他の復号データ（非暗号化データ）をセレクタステップＳ１１２に出力することを示している。

【０１３１】

ステップＳ１１０（図１１，図１２参照）では、ステップＳ１０８におけるブロックキーＫｂ１を適用した復号処理の結果、取得された復号ＴＳパケット３０４から抽出したシード情報（シード２）と、ステップＳ１０５（図１１参照）において生成した記録キーＫ２とに基づいて、ＡＥＳ暗号処理を実行し、ブロックキーＫｂ２を算出する。

【０１３２】

次に、ステップＳ１１１において、ブロックキーＫｂ２を適用してユーザデータ部の暗号化部（ブロックキーＫｂ２で暗号化されたデータ領域３４２）を復号し、復号ＴＳパケット群３０５を生成する。

【０１３３】

復号ＴＳパケット群３０５、および復号ＴＳパケット３０４は、セレクタステップＳ１１２において結合されて、復号ＴＳパケットとして例えばＭＰＥＧ２デコーダに入力され、デコードされた後、再生される。

【０１３４】

このように、本構成においては、シード情報（シード１）ユーザデータ内の先頭ＴＳパケット内に格納し、ブロックキーＫｂ２を生成するために必要となるシード情報（シード２）をユーザデータ内の第２ＴＳパケット内に格納し、シード情報（シード２）を、シード情報（シード１）と、記録キーＫ１とに基づいて生成するブロックキーＫｂ１によって暗号化して格納する構成とした。

【０１３５】

本構成においても、シード情報（シード２）をディスクから直接読み取ることは不可能である。従ってシード情報を用いて生成される鍵情報の解析、暗号アルゴリズムの解析の困難性が高まり、セキュリティレベルの高いコンテンツ保護が実現される。

【０１３６】

次に、図１３、図１４、図１５を参照してシード情報（シード１）と記録キーＫに基づいて生成するブロックキーＫｂ１によって暗号化する領域の例について説明する。図１３は、制御ブロックにシード情報（シード１）が格納され、シード情報（シード２）が、ユーザデータの１つのＴＳパケットに含まれる場合の例である。図８、図９、図１２を参照して説明した例では、シード情報（シード２）が、ユーザデータの先頭または２番目のＴＳパケット内に含まれる場合について説明したが、シード情報（シード２）は、先頭、または第２番目のＴＳパケット以外のユーザデータ部を構成する任意のＴＳパケット内に格納可能である。

【０１３７】

ユーザデータのいずれかのＴＳパケットにシード情報（シード２）を格納した場合、シード情報（シード１）と記録キーＫ１とに基づいて生成するブロックキーＫｂ１によって暗号化する領域例として、例えば図１３（ａ）～（ｃ）の構成がある。（ａ）は、シード情報（シード２）のみをブロックキーＫｂ１によって暗号化した例である。それ以外の領域は、非暗号化領域とするか、あるいは、シード情報（シード２）と記録キーＫ２によって生成されるブロックキーＫｂ２によって暗号化したデータ領域とする。

【０１３８】

（ｂ）は、シード情報（シード２）を含むＴＳパケットの一部領域をブロックキーＫｂ１によって暗号化した例である。

【０１３９】

コンテンツ編集スタジオ２８２（図６参照）においてシード情報（シード２）と編集識別子（編集ＩＤ）をＴＳパケット内に格納し、ディスク製造エンティティ２８３（図６参照）において、シード情報（シード１）に基づいて生成可能な記録キーＫ１を用いて、シード情報（シード２）の暗号化処理を行った後、ディスクに格納する。

【０１４０】

（ｃ）は、シード情報（シード２）を含む１つのＴＳパケットの全領域をブロックキーＫｂ１によって暗号化した例である。

【０１４１】

図１４に示す例は、シード情報（シード１）とシード情報（シード２）を同一のＴＳパケット内に格納した例を示している。シード情報（シード１）は非暗号化情報として格納される。シード情報（シード２）は、シード情報（シード１）と記録キーＫ１とに基づいて生成するブロックキーＫｂ１によって暗号化され、シード情報（シード１）と同一のＴＳパケット内に格納される。

【０１４２】

（ｄ）は、シード情報（シード２）のみをブロックキーＫｂ１によって暗号化した例である。それ以外の領域は、非暗号化領域とするか、あるいは、シード情報（シード２）と記録キーＫ２によって生成されるブロックキーＫｂ２によって暗号化したデータ領域とする。

【０１４３】

（ｅ）は、シード情報（シード２）を含むＴＳパケットの一部領域をブロックキーＫｂ１によって暗号化した例である。（ｆ）は、シード情報（シード２）を含む１つのＴＳパケットの全領域をブロックキーＫｂ１によって暗号化した例である。

【０１４４】

図１５に示す例は、シード情報（シード１）とシード情報（シード２）を異なるＴＳパケット内に格納した例を示している。シード情報（シード１）は非暗号化情報として格納される。シード情報（シード２）は、シード情報（シード１）と記録キーＫ１とに基づいて生成するブロックキーＫｂ１によって暗号化され、シード情報（シード１）と異なるＴＳパケット内に格納される。

【０１４５】

（ｇ）は、シード情報（シード２）のみをブロックキーＫｂ１によって暗号化した例である。それ以外の領域は、非暗号化領域とするか、あるいは、シード情報（シード２）と記録キーＫ２によって生成されるブロックキーＫｂ２によって暗号化したデータ領域とする。

【０１４６】

（ｈ）は、シード情報（シード２）を含むＴＳパケットの一部領域をブロックキーＫｂ１によって暗号化した例である。（ｉ）は、シード情報（シード２）を

含む１つのＴＳパケットの全領域をブロックキーＫｂ１によって暗号化した例である。

【０１４７】

以上、図１３～図１５を参照して説明したように、シード情報（シード１）およびシード情報（シード２）の格納態様、および暗号化データ領域の設定態様は様々な設定が可能である。しかし、いずれの場合もシード情報（シード２）は、シード情報（シード１）を用いて生成される鍵、すなわちブロックキーＫｂ１によって暗号化されて格納されるので、情報記録媒体からの直接読み取りが不可能となり、シード情報（シード２）の解析、シード情報（シード２）を適用して生成するブロックキーＫｂ２の解析、ブロックキーＫｂ２によって暗号化されるユーザデータの暗号化アルゴリズムの解析困難性を高めることが可能となる。

【０１４８】

[情報記録媒体ドライブ装置とのインタフェースを介するデータ入出力構成]

次に、ＰＣ等の情報処理装置において、様々なインタフェース、例えばＳＣＳＩ、ＩＥＥＥ１３９４、ＵＳＢ等のインタフェースを介してＤＶＤ、ＣＤ等の情報記録媒体を装着した情報記録媒体ドライブと接続し、インタフェースを介してデータ転送を実行する場合の処理例について説明する。

【０１４９】

例えば、図１５に示すように、ＰＣ等の情報処理装置４１０と、ＤＶＤ、ＣＤ等の情報記録媒体４３０を装着した情報記録媒体ドライブ４２０とを双方のインタフェース４１１，４２１を介して接続した構成であり、情報記録媒体ドライブ４２０が情報記録媒体４３０に対するアクセスを実行し、データを双方のインタフェース４１１，４２１を介して転送し、ＰＣ等の情報処理装置４１０において再生する構成である。

【０１５０】

図に示すように、インタフェース４１１，４２１を介してデータが転送される場合、転送データに上述したシード情報（シード２）が非暗号化状態で含まれると、転送データからのシード情報（シード２）の漏洩が発生する可能性がある。

【０１５１】

そこで、本発明の構成においては、情報処理装置４１０と情報記録媒体ドライブ４２０間でインタフェースを介してデータ転送が実行される場合、双方の装置間において、認証処理を実行し、認証処理の結果、双方の機器で取得するセッションキーを用いて転送データを暗号化して送信する構成とした。以下、この処理構成の詳細について説明する。

【０１５２】

図１７に、ＰＣ等の情報処理装置５００と情報記録媒体ドライブ５１０において、暗号化コンテンツを格納した情報記録媒体５２０のデータ読み出し、再生を実行する場合の処理を説明する図を示す。なお、情報処理装置５００と情報記録媒体ドライブ５１０とも、先に図２を参照して説明した構成とほぼ同様の構成を持つ。ただし、ＰＣ等の情報処理装置５００は、図２に示す記録媒体１９５およびドライブ１９０は必須ではなく、これらは、情報記録媒体ドライブ５１０のみが備えていればよい。また、ＭＰＥＧコーデック１３０、ＴＳ処理手段１９８はＰＣ等の情報処理装置５００のみが有する構成でよく、情報記録媒体ドライブ５１０には構成する必要がない。

【０１５３】

図１７を参照して、情報記録媒体５２０のデータを情報記録媒体ドライブ５１０において読み出し、情報処理装置５００に転送して再生する場合の処理を説明する。

【０１５４】

情報記録媒体ドライブ５１０は自身のメモリ１８０（図２参照）に格納しているマスターキー５１１を読み出す。なお、マスターキー５１１は、情報処理装置５００側に格納されている場合は、情報処理装置５００から情報記録媒体ドライブ５１０に送信してもよい。マスターキー５１１は、ライセンスを受けた情報処理装置（情報記録媒体ドライブを含む）に格納された秘密キーであり、複数の情報処理装置に共通なキーとして格納された共通キーである。

【０１５５】

情報記録媒体ドライブ５１０は、ディスクＩＤ（Disc ID）５２１を情報記録

媒体５２０から読出す。ディスクＩＤ（Disc ID）５２１は、ディスク固有情報であり、例えば一般データ格納領域または、リードインエリアに格納される。

【０１５６】

次に、情報記録媒体ドライブ５１０は、ステップＳ５５１において、マスターキー５１１とディスクＩＤ５２１を用いて、ディスク固有キー（Disc Unique Key）を生成する。ディスク固有キー（Disc Unique Key）の具体的な生成方法は、先に図４を参照して説明したと同様の方法が適用できる。

【０１５７】

次に、記録コンテンツごとの２つの固有鍵であるタイトルキー（Title Key）１，５２３、タイトルキー２，５２４を情報記録媒体５２０から読出す。ディスク上には、どこのデータがどんなタイトルを構成するかという情報が格納されたデータ管理ファイルがあり、このファイルにタイトルキーが格納されている。ディスク１枚に対してタイトルキーが１組しかない場合、すなわちディスクＩＤ５２１に対するタイトルキーが一意に決定できる場合には、ディスクＩＤ５２１と同様の方法で、例えば一般データ格納領域または、リードインエリアに格納するようにしてもよい。

【０１５８】

次にステップＳ５５２およびステップＳ５５３において、ディスク固有キー（Disc Unique Key）とタイトルキー（Title Key）１，２から、２つのタイトル固有キー（Title Unique Key）１，２を生成する。

【０１５９】

さらに、情報記録媒体ドライブ５１０は、ステップＳ５５２およびステップＳ５５３において生成した２つのタイトル固有キー（Title Unique Key）１，２と、情報記録媒体５２０から読み出した記録シード（ＲＥＣ　ＳＥＥＤ）５２５、物理インデックス５２６とに基づいて、ステップＳ５５４、Ｓ５５５において、２つの記録キー（ＲＥＣキー）Ｋ１，Ｋ２を生成する。

【０１６０】

ステップＳ５５２～Ｓ５５５において実行する２つの記録キー（ＲＥＣキー）Ｋ１，Ｋ２の生成処理は、先に図５を参照して説明した通り、２つのタイトル固

有キー（Title Unique Key）１，２と、情報記録媒体５２０から読み出した記録シード（ＲＥＣ　ＳＥＥＤ）５２５、物理インデックス５２６とに基づくＡＥＳ（Advanced Encryption Standard）暗号処理により生成される。

【０１６１】

なお、先に図７を参照して説明した通り、記録シード（ＲＥＣ　ＳＥＥＤ）５２５、物理インデックス５２６を情報記録媒体５２０に格納する代わりに編集（オーサリング）毎に設定される乱数等のランダム値をディスクキーシードとして情報記録媒体５２０に格納して、ディスクキーシードに対してディスク固有キーを適用して、ＡＥＳ暗号処理を実行し、その出力からタイトル固有キー１、タイトル固有キー２を得る方法としてもよい。

【０１６２】

上述のいずれかの方法により、ステップＳ５５４、Ｓ５５５において２つの記録キー（ＲＥＣキー）１，２を生成すると、次に、ステップＳ５５６において、ブロックキーＫｂ１の生成処理を実行する。

【０１６３】

ブロックキーＫｂ１の生成処理においては、情報記録媒体５２０からブロックキーＫｂ１生成情報としてのシード情報（シード１）５２７を読み出し、シード情報（シード１）５２７と、ステップＳ５５４において生成した記録キーＫ１とに基づく暗号処理を実行してブロックキーＫｂ１を生成する。

【０１６４】

ステップＳ５５６のブロックキーＫｂ１の生成処理以降に実行する処理について、図１８を参照して説明する。

【０１６５】

図１８において、復号処理は、図８～図１２を参照して説明したと同様、処理単位６００を単位として実行される。この処理単位は、先に図１を参照して説明した（ｂ）処理単位に相当する。すなわち、暗号処理単位である１ユニット（１ＡＵ：Aligned Unit）である。情報記録媒体５２０に格納された暗号化データの読み取りを実行する情報記録媒体ドライブ５１０は、制御データ内のフラグに基づいて、暗号処理単位である１ＡＵ（Aligned Unit）を抽出する。

【０１６６】

処理単位６００には、１８バイトの制御データ６０１と、６１４４バイトのユーザデータ（暗号化コンテンツを含む）が含まれる。６１４４バイトのユーザデータは、トランスポートストリームパケットの単位である１９２バイト毎に分割される。ユーザデータの先頭のＴＳパケット６０２と、後続の５９５２バイトのＴＳパケット群６０３を分離して説明する。この例では、シード情報（シード１）６１１が制御データ６０１に格納され、シード情報（シード２）６１２がユーザデータ内の先頭のＴＳパケット６０２内に暗号化されて格納された例である。

【０１６７】

なお、シード情報としての、シード１、シード２の格納態様には複数の態様があり、ここではその一例を示す。他の例については、後段で説明する。

【０１６８】

図１８において、図１７の処理ステップと同様の処理ステップには、同一の処理ステップ番号を付してある。

【０１６９】

ステップＳ５５６（図１７、図１８）は、情報記録媒体の制御データ内から読み出したシード情報（シード１）６１１をＡＥＳ暗号処理部に入力し、先のステップＳ５５４において生成した記録キーＫｂ１を適用したＡＥＳ暗号処理を実行しブロックキーＫｂ１生成処理を実行するステップである。

【０１７０】

次に、図１７のステップＳ５５７において、３２ＴＳパケットからなるユーザデータからブロックキーＫｂ１による暗号化データ部のみが抽出される。ブロックキーＫｂ１による暗号化データ部、非暗号化部がステップＳ５５７において分離されて、暗号化部のみがステップＳ５５８において復号される。非暗号化部は、ステップＳ５５８をスキップし、ステップＳ５５９において、再度セレクタステップにより復号データと連結され、ステップＳ５６３においてセッションキーによって暗号化がなされる。

【０１７１】

ステップＳ５５８（図１７、図１８参照）では、ステップＳ５５６において生

成したブロックキーＫｂ１を適用したＡＥＳ復号処理を実行する。ステップＳ５５８では、ブロックキーＫｂ１を適用した暗号処理のなされたデータ部のみを対象とした復号処理が実行される。この例では、ユーザデータの先頭ＴＳパケット６０２の少なくともシード情報（シード２）を含むデータ領域がブロックキーＫｂ１を適用した暗号処理のなされたデータ部である。従って、このシード情報（シード２）を含むデータ領域を対象としてブロックキーＫｂ１を適用した復号処理を実行する。

【０１７２】

なお、ブロックキーＫｂ１を適用した暗号処理のなされたデータ部をどのデータ領域とするかについては、いくつかのパターンがあり、これらについては、先に、図１３～図１５を参照して説明した通りである。

【０１７３】

先頭ＴＳパケット６０２には、他のユーザデータ部、すなわち、後続の５９５２バイトのＴＳパケット群６０３の復号処理に適用するブロックキーＫｂ２を算出するために必要となるシード情報（シード２）６１２が含まれている。すなわち、シード情報（シード２）６１２は、ブロックキーＫｂ１を適用した暗号処理がなされた暗号化データとして先頭ＴＳパケット６０２に記録されている。

【０１７４】

ステップＳ５５６における、ブロックキーＫｂ１を適用した復号処理の結果として、復号ＴＳパケット６０４が算出され、その中には、シード情報（シード２）が含まれる。

【０１７５】

図１７のセレクタステップＳ５５９は、ブロックキーＫｂ１を適用した復号処理の結果から、シード情報（シード２）を含む復号データと、その他のデータを結合して、暗号化ステップＳ５６３に出力することを示している。

【０１７６】

ステップＳ５６３における暗号化処理は、情報記録媒体ドライブ５１０と、情報処理装置５００との間で実行する相互認証処理の結果として双方で共有するセッションキーに基づいて実行する暗号処理である。相互認証処理は、情報記録媒

体ドライブ５１０と、情報処理装置５００とが共有する認証キーＫｍ５３０，５４０に基づいて実行される。

【０１７７】

相互認証処理のシーケンスについて、図１９を参照して説明する。図１９に示す認証およびセッションキー共有処理は、共通鍵処理方式に基づく一例である。認証シーケンスおよびセッションキー共有シーケンスは、この処理シーケンスに限らず、他の処理方法を適用してもよい。

【０１７８】

情報記録媒体ドライブ５１０と、情報処理装置５００は認証キーＫｍ５３０，５４０を有する。まず、ステップＳ５７１において、情報処理装置５００が乱数Ｒｂ１（６４ｂｉｔ）を生成し、情報記録媒体ドライブ５１０に送信する。情報記録媒体ドライブ５１０は、ステップＳ５８１において、乱数Ｒａ１を生成し、ステップＳ６８２において、乱数Ｒａ１と乱数Ｒｂ１の結合データ［Ｒａ１‖Ｒｂ１］に対するＡＥＳ暗号化処理に基づくＭＡＣ（Message Authentication Code）を生成する。生成ＭＡＣ値をｅＫｍ（Ｒａ１‖Ｒｂ１）とする。なお、ｅＫａ（Ｂ）は、キーＫａによるデータＢの暗号化を示し、Ａ‖Ｂは、データＡとデータＢの連結を示す。情報記録媒体ドライブ５１０は、生成ＭＡＣ値：ｅＫｍ（Ｒａ１‖Ｒｂ１）と、生成乱数Ｒａ１を情報処理装置５００に送信する。

【０１７９】

情報処理装置５００は、情報記録媒体ドライブ５１０から受信した乱数Ｒａ１とステップＳ５７１において生成した乱数Ｒｂ１とに基づいて、ステップＳ５７２において、ＭＡＣ値：ｅＫｍ（Ｒａ１‖Ｒｂ１）を算出する。さらに、ステップＳ５７３において、算出したＭＡＣ値と、情報記録媒体ドライブ５１０から受信したＭＡＣ値とを比較する。一致すれば、情報処理装置５００は、情報記録媒体ドライブ５１０が正しい認証キーを持つ正規なデバイスであると認証する。不一致の場合は、認証エラーであり、その後の処理を中止する。

【０１８０】

さらに、情報処理装置５００は、ステップＳ５７４において、乱数Ｒｂ２を生成し、情報記録媒体ドライブ５１０に送信する。情報記録媒体ドライブ５１０は

、ステップＳ５８３において、乱数Ｒａ２を生成し、生成乱数Ｒａ２を情報処理装置５００に送信する。

【０１８１】

情報処理装置５００は、ステップＳ５７５において、受信乱数Ｒａ２と生成乱数Ｒｂ２とに基づいて、ＭＡＣ値：ｅＫｍ（Ｒａ２‖Ｒｂ２）を算出し、情報記録媒体ドライブ５１０に送信する。

【０１８２】

情報記録媒体ドライブ５１０は、ステップＳ５８４において、受信した乱数Ｒｂ２とステップＳ５８３において生成した乱数Ｒａ２とに基づいて、ＭＡＣ値：ｅＫｍ（Ｒａ２‖Ｒｂ２）を算出する。さらに、ステップＳ５８５において、算出したＭＡＣ値と、情報処理装置５００から受信したＭＡＣ値とを比較する。一致すれば、情報記録媒体ドライブ５１０は、情報処理装置５００が正しい認証キーを持つ正規なデバイスであると認証する。不一致の場合は、認証エラーであり、その後の処理を中止する。

【０１８３】

さらに、情報処理装置５００は、ステップＳ５７６において、乱数Ｒａ３を生成して情報記録媒体ドライブ５１０に送信する。

【０１８４】

情報記録媒体ドライブ５１０は、ステップＳ５８６において、乱数Ｒａ３を生成し、ステップＳ５８７において、生成乱数Ｒａ３と情報処理装置５００からの受信乱数Ｒｂ３との連結データ対する共有認証キーＫｍを適用したＡＥＳ暗号処理を実行し、セッションキーＫｓ＝ｅＫｍ（Ｒａ３‖Ｒｂ３）を算出する。

【０１８５】

情報処理装置５００は、ステップＳ５７７において、生成乱数Ｒｂ３と情報記録媒体ドライブ５１０からの受信乱数Ｒａ３との連結データに対する共有認証キーＫｍを適用したＡＥＳ暗号処理を実行し、セッションキーＫｓ＝ｅＫｍ（Ｒａ３‖Ｒｂ３）を算出する。

【０１８６】

上述した処理により、情報処理装置５００と情報記録媒体ドライブ５１０とは

、相互に正しいデバイスであることを確認し、セッションキーＫｓ＝ｅＫｍ（Ｒａ３‖Ｒｂ３）を共有することができる。図１７に示すステップＳ５６０、Ｓ５６１の処理が図１９を参照して説明した処理に対応する。

【０１８７】

上述した処理によって、セッションキーＫｓが情報処理装置５００と情報記録媒体ドライブ５１０とによって共有されると、図１７に示すステップＳ５６２、Ｓ５６３の暗号化処理が情報記録媒体ドライブ５１０によって実行される。

【０１８８】

ステップＳ５６２の暗号化処理は、ステップＳ５５５において生成した記録キーＫ２をセッションキーＫｓで暗号化（ＡＥＳ暗号化）し、暗号化記録キーｅＫｓ（Ｋ２）を生成する処理である。ステップＳ５６３は、ステップＳ５５８におけるブロックキーＫｂ１を適用した復号処理の結果取得された復号ＴＳパケット６０４をセッションキーＫｓによって暗号化する処理である。なお、この場合、暗号化する対象は、ＴＳパケット６０４全体である場合、一部である場合、シード情報（シード２）のみである場合など、処理態様は、ＴＳパケットに含まれる秘密にすべき情報の格納態様、すなわちブロックキーＫｂ１によって暗号化された範囲に応じて決定してよい。これらの各態様は、図１３～図１５を参照して説明したとおりである。

【０１８９】

ステップＳ５６２において、記録キーＫ２のセッションキーＫｓによる暗号化データが生成され、ステップＳ５６３において、シード情報（シード２）を含む秘密情報がセッションキーＫｓによって暗号化され、これらの暗号化データ（図１８のＴＳパケット６０５）が情報記録媒体ドライブ５１０から、情報処理装置５００に送信される。すなわち、データ通信路において、転送されるデータはセッションキーＫｓによって暗号化されたデータとなる。

【０１９０】

情報処理装置５００は、情報記録媒体ドライブ５１０から、これらのデータを受信すると、ステップＳ５６４およびステップＳ５６５において、受信暗号化データを復号する。すなわち、ステップＳ５６４において、セッションキーＫｓを

適用して暗号化記録キーｅＫｓ（Ｋ２）を復号して記録キーＫ２を取得し、ステップＳ５６５において、セッションキーＫｓを適用してシード情報（シード２）を含む秘密情報を復号してシード情報（シード２）を含む秘密情報を取得する。図１８に示すＴＳパケット６０６が復号されたシード情報（シード２）を含む。

【０１９１】

ステップＳ５６６は、復号されたシード情報（シード２）と、ブロックキーＫｂ２による復号対象データと、非暗号化データとを分離するセレクタステップである。ステップＺＳ５６７（図１７，図１８参照）では、ステップＳ５６５におけるセッションキーＫｓを適用した復号処理の結果取得されたシード情報（シード２）と、ステップＳ５６４において生成した記録キーＫ２とに基づいて、ＡＥＳ暗号処理を実行し、ブロックキーＫｂ２を算出する。

【０１９２】

次に、ステップＳ５６８において、ブロックキーＫｂ２を適用してユーザデータ部の暗号化部（ブロックキーＫｂ２で暗号化されたデータ領域）を復号し、復号ＴＳパケット群６０７を生成する。

【０１９３】

復号ＴＳパケット群６０７、および復号ＴＳパケット６０６は、セレクタステップＳ５６９において結合されて、復号ＴＳパケットとして例えばＭＰＥＧ２デコーダに入力され、デコードされた後、再生される。

【０１９４】

このように、本構成においては、情報記録媒体に格納されたデータの再生処理において、暗号化コンテンツの復号に適用する鍵（ブロックキーＫｂ２）を生成するために必要となるシード情報（シード２）をデバイス間で転送することが必要となる構成において、ブロックキーＫｂ２の生成に必要となるシード情報（シード２）および記録キーＫ２の双方をセッションキーで暗号化して送受信する構成としたので、転送路からのデータ漏洩が発生した場合であっても、シード情報（シード２）および記録キーＫ２を取得することは困難であり、従ってシード情報を用いて生成される鍵情報の解析、暗号アルゴリズムの解析の困難性が高まり、セキュリティレベルの高いコンテンツ保護が実現される。これは、情報処理装

置５００の中で、例えば記録キーＫ１の取得方法からブロックキーＫｂ１の算出方法、そして、セッションキーＫｓの生成方法、および、セッションキーＫｓによる暗号化方法を一つのＬＳＩパッケージ内の処理として秘匿性を高めることによって、一層強固なものとなる。

【０１９５】

なお、前述した例と同様、２つのシード情報の格納形態には、様々な態様があり、以下、複数の例について説明する。

【０１９６】

図２０に、シード情報（シード１）と、シード情報（シード２）とを共にユーザデータ内の先頭ＴＳパケット６０２内に格納した例を示す。先に図１８を参照して説明した例では、シード情報（シード１）６１１が制御データ６０１に格納され、シード情報（シード２）６１２がユーザデータ内の先頭のＴＳパケット６０２内に暗号化されて格納された例を説明したが、図２０に示す構成例は、シード情報（シード１）６２１、シード情報（シード２）６２２、双方がユーザデータ内の先頭のＴＳパケット６０２内に格納された例である。

【０１９７】

なお、シード情報（シード２）６２２は、図１８において説明した例と同様、シード情報（シード１）６２１を適用して取得されるブロックキーＫｂ１によって暗号化されてユーザデータ内の先頭のＴＳパケット６０２内に格納される。

【０１９８】

図２０において、復号処理は、処理単位６００を単位として実行される。この処理単位は、先に図１を参照して説明した（ｂ）処理単位に相当する１ユニット（１ＡＵ：Aligned Unit）である。情報記録媒体５２０に格納された暗号化データの読み取りを実行する情報記録媒体ドライブ５１０は、制御データ内のフラグに基づいて、暗号処理単位である１ＡＵ（Aligned Unit）を抽出する。

【０１９９】

図２０の処理について説明する。図２０において、図１７の処理ステップと同様の処理ステップには、同一の処理ステップ番号を付してある。

【０２００】

ステップＳ５５６（図１７、図２０）は、情報記録媒体のユーザデータの先頭ＴＳパケット内から読み出したシード情報（シード１）６２１をＡＥＳ暗号処理部において、先のステップＳ５５４（図１７参照）において生成した記録キーＫ１を適用したＡＥＳ暗号処理を実行しブロックキーＫｂ１生成処理を実行する。

【０２０１】

次に、図１７のステップＳ５５７において、３２ＴＳパケットからなるユーザデータからブロックキーＫｂ１による暗号化データ部のみが抽出される。ブロックキーＫｂ１による暗号化データ部、非暗号化部がステップＳ５５７において分離されて、暗号化部のみがステップＳ５５８において復号される。非暗号化部は、ステップＳ５５８をスキップし、ステップＳ５５９において、再度セレクタステップにより復号データと連結され、ステップＳ５６３においてセッションキーによって暗号化がなされる。

【０２０２】

ステップＳ５５８（図１７、図２０参照）では、ステップＳ５５６において生成したブロックキーＫｂ１を適用したＡＥＳ復号処理を実行する。ステップＳ５５８では、ブロックキーＫｂ１を適用した暗号処理のなされたデータ部のみを対象とした復号処理が実行される。この例では、ユーザデータの先頭ＴＳパケット６０２の少なくともシード情報（シード２）を含むデータ領域がブロックキーＫｂ１を適用した暗号処理のなされたデータ部である。従って、このシード情報（シード２）を含むデータ領域を対象としてブロックキーＫｂ１を適用した復号処理を実行する。

【０２０３】

この先頭ＴＳパケット６０２の暗号化データ領域には、他のユーザデータ部、すなわち、後続の５９５２バイトのＴＳパケット群６０３の復号処理に適用するブロックキーＫｂ２を算出するために必要となるシード情報（シード２）６２２が含まれている。すなわち、シード情報（シード２）６２２は、ブロックキーＫｂ１を適用した暗号処理がなされた暗号化データとして先頭ＴＳパケット６０２に記録されている。

【０２０４】

ステップＳ５５６における、ブロックキーＫｂ１を適用した復号処理の結果として、復号ＴＳパケット６０４が算出され、その中にはシード情報（シード２）が含まれる。

【０２０５】

図１７のセレクタステップＳ５５９は、ブロックキーＫｂ１を適用した復号処理の結果から、シード情報（シード２）を含む復号データと、その他のデータを結合して、暗号化ステップＳ５６３に出力することを示している。

【０２０６】

ステップＳ５６３における暗号化処理は、情報記録媒体ドライブ５１０と、情報処理装置５００との間で実行する相互認証処理の結果として双方で共有するセッションキーに基づいて実行する暗号処理である。相互認証処理は、情報記録媒体ドライブ５１０と、情報処理装置５００とが共有する認証キーＫｍ５３０，５４０に基づいて実行される。相互認証処理およびセッションキー共有処理は、図１９を参照して説明した通りである。

【０２０７】

認証が成立し、セッションキーＫｓが共有されると、図１７、図２０に示すステップＳ５６２、Ｓ５６３の暗号化処理が情報記録媒体ドライブ５１０によって実行される。すなわち、ステップＳ５６２において、記録キーＫ２のセッションキーＫｓによる暗号化データが生成され、ステップＳ５６３において、シード情報（シード２）を含む秘密情報がセッションキーＫｓによって暗号化され、これらの暗号化データ（図２０のＴＳパケット６０５）が情報記録媒体ドライブ５１０から、情報処理装置５００に送信される。すなわち、データ通信路において、転送されるデータはセッションキーＫｓによって暗号化されたデータとなる。

【０２０８】

情報処理装置５００は、情報記録媒体ドライブ５１０から、これらのデータを受信すると、ステップＳ５６４およびステップＳ５６５において、受信暗号化データを復号する。すなわち、ステップＳ５６４において、セッションキーＫｓを適用して暗号化記録キーｅＫｓ（Ｋ２）を復号して記録キーＫ２を取得し、ステップＳ５６５において、セッションキーＫｓを適用してシード情報（シード２）

を含む秘密情報を復号してシード情報（シード２）を含む秘密情報を取得する。図２０に示すＴＳパケット６０６が復号されたシード情報（シード２）を含む。

【０２０９】

ステップＳ５６６は、復号されたシード情報（シード２）と、ブロックキーＫｂ２による復号対象データと、非暗号化データとを分離するセレクタステップである。ステップＺＳ５６７（図１７，図２０参照）では、ステップＳ５６５におけるセッションキーＫｓを適用した復号処理の結果取得されたシード情報（シード２）と、ステップＳ５６４において生成した記録キーＫ２とに基づいて、ＡＥＳ暗号処理を実行し、ブロックキーＫｂ２を算出する。

【０２１０】

次に、ステップＳ５６８において、ブロックキーＫｂ２を適用してユーザデータ部の暗号化部（ブロックキーＫｂ２で暗号化されたデータ領域）を復号し、復号ＴＳパケット群６０７を生成する。

【０２１１】

復号ＴＳパケット群６０７、および復号ＴＳパケット６０６は、セレクタステップＳ５６９において結合されて、復号ＴＳパケットとして例えばＭＰＥＧ２デコーダに入力され、デコードされた後、再生される。

【０２１２】

このように、本構成においては、シード情報（シード１）と、シード情報（シード２）とを共にユーザデータ内の先頭ＴＳパケット内に格納し、ブロックキーＫｂ２を生成するために必要となるシード情報（シード２）は、シード情報（シード１）と、記録キーＫ１とに基づいて生成するブロックキーＫｂ１によって暗号化して格納する構成とした。

【０２１３】

本構成においても、シード情報（シード２）のディスクからの直接読み取り、データ転送路からの読み取りを行うことは不可能であり、従ってシード情報を用いて生成される鍵情報の解析、暗号アルゴリズムの解析の困難性が高まり、セキュリティレベルの高いコンテンツ保護が実現される。これは、情報処理装置５００の中で、例えば記録キーＫ１の取得方法からブロックキーＫｂ１の算出方法、

そして、セッションキーＫｓの生成方法、および、セッションキーＫｓによる暗号化方法を一つのＬＳＩパッケージ内の処理として秘匿性を高めることによって、一層強固なものとなる。

【０２１４】

図２１に示す例は、シード情報（シード１）６３１をユーザデータ内の先頭ＴＳパケット６０２に格納し、シード情報（シード２）６３２をユーザデータ内の次のＴＳパケット６４１に格納した例である。

【０２１５】

なお、シード情報（シード２）６３２は、図１８、図２０において説明した例と同様、シード情報（シード１）６３１を適用して取得されるブロックキーＫｂ１によって暗号化されてユーザデータ内の第２のＴＳパケット６４１内に格納される。

【０２１６】

図２１において、復号処理は、処理単位６００を単位として実行される。この処理単位は、先に図１を参照して説明した（ｂ）処理単位に相当する１ユニット（１ＡＵ：Aligned Unit）である。

【０２１７】

図２１の処理について説明する。図２１において、図１７の処理ステップと同様の処理ステップには、同一の処理ステップ番号を付してある。

【０２１８】

ステップＳ５５６（図１７、図２１）は、情報記録媒体のユーザデータの先頭ＴＳパケット内から読み出したシード情報（シード１）６３１をＡＥＳ暗号処理部に入力し、先のステップＳ５５４（図１７参照）において生成した記録キーＫ１を適用したＡＥＳ暗号処理を実行してブロックキーＫｂ１を生成する。

【０２１９】

次に、図１７のステップＳ５５７において、３２ＴＳパケットからなるユーザデータからブロックキーＫｂ１による暗号化データ部のみが抽出される。ブロックキーＫｂ１による暗号化データ部、非暗号化部がステップＳ５５７において分離されて、暗号化部のみがステップＳ５５８において復号される。非暗号化部は

、ステップＳ５５８をスキップし、ステップＳ５５９において、再度セレクタステップにより復号データと連結され、ステップＳ５６３においてセッションキーによって暗号化がなされる。

【０２２０】

ステップＳ５５８（図１７、図２１参照）では、ステップＳ５５６において生成したブロックキーＫｂ１を適用したＡＥＳ復号処理を実行する。復号処理対象は、ブロックキーＫｂ１を適用した暗号処理がなされているデータ領域であり、ユーザデータの先頭ＴＳパケット中のシード情報（シード１）５２１を除くデータ領域の暗号化領域と、第２ＴＳパケット中の少なくともシード情報（シード２）６３２を含むデータ領域の復号処理が実行される。ブロックキーＫｂ１を適用した暗号処理のなされたデータ部をどのデータ領域とするかについては、いくつかのパターンがあり、これらについては前述した通りである。

【０２２１】

本例では、第２のＴＳパケット６４１の暗号化データ領域に、他のユーザデータ部、すなわち、後続のＴＳパケット群６４２の復号処理に適用するブロックキーＫｂ２を算出するために必要となるシード情報（シード２）６３２が含まれる。すなわち、シード情報（シード２）６３２は、ブロックキーＫｂ１を適用した暗号処理がなされた暗号化データとして第２ＴＳパケット６４１に記録されている。

【０２２２】

ステップＳ６０６における、ブロックキーＫｂ１を適用した復号処理の結果として、復号ＴＳパケット６０４が算出される。その中にシード情報（シード２）が含まれる。

【０２２３】

図１７のセレクタステップＳ５５９は、ブロックキーＫｂ１を適用した復号処理の結果から、シード情報（シード２）を含む復号データと、その他のデータを結合して、暗号化ステップＳ５６３に出力することを示している。

【０２２４】

ステップＳ５６３における暗号化処理は、情報記録媒体ドライブ５１０と、情

報処理装置５００との間で実行する相互認証処理の結果として双方で共有するセッションキーに基づいて実行する暗号処理である。相互認証処理は、情報記録媒体ドライブ５１０と、情報処理装置５００とが共有する認証キーＫｍ５３０，５４０に基づいて実行される。相互認証処理およびセッションキー共有処理は、図１９を参照して説明した通りである。

【０２２５】

認証が成立し、セッションキーＫｓが共有されると、図１７、図２１に示すステップＳ５６２、Ｓ５６３の暗号化処理が情報記録媒体ドライブ５１０によって実行される。すなわち、ステップＳ５６２において、記録キーＫ２のセッションキーＫｓによる暗号化データが生成され、ステップＳ５６３において、シード情報（シード２）を含む秘密情報がセッションキーＫｓによって暗号化され、これらの暗号化データ（図２１のＴＳパケット６０５）が情報記録媒体ドライブ５１０から、情報処理装置５００に送信される。すなわち、データ通信路において、転送されるデータはセッションキーＫｓによって暗号化されたデータとなる。

【０２２６】

情報処理装置５００は、情報記録媒体ドライブ５１０から、これらのデータを受信すると、ステップＳ５６４およびステップＳ５６５において、受信暗号化データを復号する。すなわち、ステップＳ５６４において、セッションキーＫｓを適用して暗号化記録キーｅＫｓ（Ｋ２）を復号して記録キーＫ２を取得し、ステップＳ５６５において、セッションキーＫｓを適用してシード情報（シード２）を含む秘密情報を復号してシード情報（シード２）を含む秘密情報を取得する。図２１に示すＴＳパケット６０６が復号されたシード情報（シード２）を含む。

【０２２７】

ステップＳ５６６は、復号されたシード情報（シード２）と、ブロックキーＫｂ２による復号対象データと、非暗号化データとを分離するセレクタステップである。ステップＺＳ５６７（図１７，図２１参照）では、ステップＳ５６５におけるセッションキーＫｓを適用した復号処理の結果取得されたシード情報（シード２）と、ステップＳ５６４において生成した記録キーＫ２とに基づいて、ＡＥＳ暗号処理を実行し、ブロックキーＫｂ２を算出する。

【０２２８】

次に、ステップＳ５６８において、ブロックキーＫｂ２を適用してユーザデータ部の暗号化部（ブロックキーＫｂ２で暗号化されたデータ領域）を復号し、復号ＴＳパケット群６０７を生成する。

【０２２９】

復号ＴＳパケット群６０７、および復号ＴＳパケット６０６は、セレクタステップＳ５６９において結合されて、復号ＴＳパケットとして例えばＭＰＥＧ２デコーダに入力され、デコードされた後、再生される。

【０２３０】

このように、本構成においては、シード情報（シード１）ユーザデータ内の先頭ＴＳパケット内に格納し、ブロックキーＫｂ２を生成するために必要となるシード情報（シード２）をユーザデータ内の第２ＴＳパケット内に格納し、シード情報（シード２）を、シード情報（シード１）と、記録キーＫ１とに基づいて生成するブロックキーＫｂ１によって暗号化して格納する構成とした。

【０２３１】

本構成においても、シード情報（シード２）をディスクから直接読み取ること、データ転送路からの読み取りを行うことは不可能であり、従ってシード情報を用いて生成される鍵情報の解析、暗号アルゴリズムの解析の困難性が高まり、セキュリティレベルの高いコンテンツ保護が実現される。これは、情報処理装置５００の中で、例えば記録キーＫ１の取得方法からブロックキーＫｂ１の算出方法、そして、セッションキーＫｓの生成方法、および、セッションキーＫｓによる暗号化方法を一つのＬＳＩパッケージ内の処理として秘匿性を高めることによって、一層強固なものとなる。

【０２３２】

[他のデータ構成における適用]

上述した例では、情報記録媒体に格納するデータをＴＳパケットとした例を説明したが、本発明の構成は、ＴＳパケット以外の様々なデータ構成においても適用可能である。すなわち、暗号化データをブロック単位で暗号化するための第２のシード情報（シード２）を、他のシード情報（シード１）を適用して生成する

ブロックキーＫｂ１によって暗号化して情報記憶媒体に格納する構成により、第２のシード情報（シード２）の漏洩が防止され、セキュリティの高いコンテンツ保護が実現される。これは、トランスポートストリーム以外のデータ構成とした場合もブロック単位の暗号化処理を適用し、シード情報を用いたブロックキーを生成する構成であれば有効となる。

【０２３３】

また、インタフェースを介したデータ転送の際にセッションキーによるデータ暗号化を行う構成例において、上述した例では、２つのシード情報中、一方をセッションキーによって暗号化する処理例を説明したが、セッションキーによるデータ暗号化を伴うデータ転送処理は、上述した構成例に限らず、一般的な暗号化コンテンツ格納構成においても有効である。

【０２３４】

暗号化されていないシード情報を記録媒体上に持つ構成において、情報処理装置と、情報記録媒体ドライブ間で、データ転送を実行する処理例について、図２２を参照して説明する。

【０２３５】

図２２に示す処理例において、情報記録媒体６７０には、暗号化コンテンツ６７５が記録され、暗号化コンテンツ６７５は、処理単位毎に設定されるシード情報６７４によって生成されるブロックキーＫｂ１で暗号化されて記録されている。

【０２３６】

情報記録媒体ドライブ６６０において、暗号化コンテンツを格納した情報記録媒体６７０のデータを読み出し、ＰＣ等の情報処理装置６５０において再生する場合の処理を説明する。

【０２３７】

情報記録媒体ドライブ６６０は自身のメモリに格納しているマスターキー６６１を読み出す。なお、マスターキー６６１は、情報処理装置６５０側に格納されている場合は、情報処理装置６５０から情報記録媒体ドライブ６６０に送信してもよい。マスターキー６６１は、ライセンスを受けた情報処理装置（情報記録媒

体ドライブを含む）に格納された秘密キーであり、複数の情報処理装置に共通なキーとして格納された共通キーである。

【０２３８】

情報記録媒体ドライブ６６０は、ディスクＩＤ（Disc ID）６７１を情報記録媒体６７０から読出す。ディスクＩＤ（Disc ID）６７１は、ディスク固有情報であり、例えば一般データ格納領域または、リードインエリアに格納される。

【０２３９】

次に、情報記録媒体ドライブ６６０は、ステップＳ６５１において、マスターキー６６１とディスクＩＤ６７１を用いて、ディスク固有キー（Disc Unique Key）を生成する。ディスク固有キー（Disc Unique Key）の具体的な生成方法は、先に図４を参照して説明したと同様の方法が適用できる。

【０２４０】

次に、記録コンテンツごとの固有鍵であるタイトルキー（Title Key）１，６７２を情報記録媒体６７０から読出す。ディスク上には、どこのデータがどんなタイトルを構成するかという情報が格納されたデータ管理ファイルがあり、このファイルにタイトルキーが格納されている。

【０２４１】

次にステップＳ６５２において、ディスク固有キー（Disc Unique Key）とタイトルキー（Title Key）１，６７２から、タイトル固有キー（Title Unique Key）１を生成する。

【０２４２】

さらに、情報記録媒体ドライブ６６０は、ステップＳ６５２において生成したタイトル固有キー（Title Unique Key）１と、情報記録媒体６７０から読み出した物理インデックス６７３とに基づいて、ステップＳ６５３において、記録キー（ＲＥＣキー）Ｋ１を生成する。

【０２４３】

ステップＳ６５３において実行する記録キー（ＲＥＣキー）Ｋ１の生成処理は、先に図５を参照して説明した通り、タイトル固有キー（Title Unique Key）１と、情報記録媒体６７０から読み出した物理インデックス６７３とに基づくＡＥ

S（Advanced Encryption Standard）暗号処理により生成される。

【０２４４】

ステップＳ６５４のブロックキーＫｂ１の生成処理においては、情報記録媒体６７０からブロックキーＫｂ１生成情報としてのシード情報６７４を読み出し、シード情報６７４と、ステップＳ６５３において生成した記録キーＫ１とに基づく暗号処理を実行してブロックキーＫｂ１を生成する。

【０２４５】

ステップＳ６５４のブロックキーＫｂ１の生成処理以降に実行する処理について、図２３を参照して説明する。

【０２４６】

図２３において、復号処理は、例えば２０４８バイトの処理単位内のユーザデータ７０１を単位として実行される。処理単位毎に制御データ７１１が設定される。情報記録媒体ドライブ６６０は、制御データ内のフラグに基づいて、暗号処理単位である１ＡＵ（Aligned Unit）を抽出する。

【０２４７】

処理単位には、１８バイトの制御データ７１１と、２０４８バイトの暗号化ユーザデータ７０１が含まれる。シード情報６７４が制御データ７１１内に格納されている。暗号化ユーザデータ７０１は、シード情報７２１に基づいて生成されるブロックキーＫｂ１によって暗号化されたデータである。

【０２４８】

図２３において、図２２の処理ステップと同様の処理ステップには、同一の処理ステップ番号を付してある。

【０２４９】

ステップＳ６５４（図２２、図２３）は、情報記録媒体の制御データ内から読み出したシード情報６７４をＡＥＳ暗号処理部に入力し、先のステップＳ６５３において生成した記録キーＫ１を適用したＡＥＳ暗号処理を実行しブロックキーＫｂ１生成処理を実行するステップである。

【０２５０】

ステップＳ６５５（図２２、図２３参照）では、ステップＳ６５４において生

成したブロックキーＫｂ１を適用したＡＥＳ復号処理を実行する。ステップＳ６５５では、ブロックキーＫｂ１を適用した暗号処理のなされたユーザデータ７０１を対象とした復号処理が実行される。例えばＡＥＳのＣＢＣ（Cipher Block Chaining）モードを適用した処理を実行する。

【０２５１】

次のステップＳ６６３における暗号化処理は、情報記録媒体ドライブ６６０と、情報処理装置６５０との間で実行する相互認証処理の結果として双方で共有するセッションキーに基づいて実行する暗号処理である。相互認証処理は、情報記録媒体ドライブ６６０と、情報処理装置６５０とが共有する認証キーＫｍ６８０，６９０に基づいて実行される。相互認証処理のシーケンスは、例えば先に図１９を参照して説明したシーケンスに従って実行される。

【０２５２】

図２２に示すステップＳ６６１、Ｓ６６２において、相互認証処理、セッションキーＫｓ生成が実行され、情報処理装置６５０と情報記録媒体ドライブ６６０とによってセッションキーＫｓが共有される。

【０２５３】

次に、ステップＳ６６３（図２２、図２３参照）の暗号化処理が情報記録媒体ドライブ６６０によって実行される。

【０２５４】

ステップＳ６６３の暗号化処理は、ステップＳ６５５において復号処理の結果取得された復号ユーザデータをセッションキーＫｓによって暗号化する処理である。例えばＡＥＳのＣＢＣ（Cipher Block Chaining）モードを適用した暗号化処理を実行し、暗号化ユーザデータ７０２を生成する。

【０２５５】

この暗号化データ（図２３のユーザデータ７０２）が情報記録媒体ドライブ６６０から、情報処理装置６５０に送信される。すなわち、データ通信路において、転送されるデータはセッションキーＫｓによって暗号化されたデータとなる。

【０２５６】

情報処理装置６５０は、情報記録媒体ドライブ６６０から、暗号化ユーザデー

タを受信すると、ステップＳ６６４において、受信暗号化データを復号する。すなわち、セッションキーＫｓを適用して例えばＡＥＳのＣＢＣ（Cipher Block Chaining）モードを適用した復号処理を実行し、ユーザデータ７０３を取得する。

【０２５７】

この例においても、情報記録媒体に格納されたデータの再生処理において、デバイス間の転送データをセッションキーで暗号化して送受信する構成としたので、転送路において盗聴等が発生した場合であっても、コンテンツの漏洩は防止され、セキュリティレベルの高いコンテンツ保護が実現される。これは、情報処理装置５００の中で、例えば記録キーＫ１の取得方法からブロックキーＫｂ１の算出方法、そして、セッションキーＫｓの生成方法、および、セッションキーＫｓによる暗号化方法を一つのＬＳＩパッケージ内の処理として秘匿性を高めることによって、一層強固なものとなる。

【０２５８】

以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

【０２５９】

なお、明細書中において説明した一連の処理はハードウェア、またはソフトウェア、あるいは両者の複合構成によって実行することが可能である。ソフトウェアによる処理を実行する場合は、処理シーケンスを記録したプログラムを、専用のハードウェアに組み込まれたコンピュータ内のメモリにインストールして実行させるか、あるいは、各種処理が実行可能な汎用コンピュータにプログラムをインストールして実行させることが可能である。

【０２６０】

例えば、プログラムは記録媒体としてのハードディスクやＲＯＭ（Read Only Memory）に予め記録しておくことができる。あるいは、プログラムはフレキシブ

ルディスク、ＣＤ－ＲＯＭ(Compact Disc Read Only Memory)，ＭＯ(Magneto optical)ディスク，ＤＶＤ(Digital Versatile Disc)、磁気ディスク、半導体メモリなどのリムーバブル記録媒体に、一時的あるいは永続的に格納（記録）しておくことができる。このようなリムーバブル記録媒体は、いわゆるパッケージソフトウエアとして提供することができる。

【０２６１】

なお、プログラムは、上述したようなリムーバブル記録媒体からコンピュータにインストールする他、ダウンロードサイトから、コンピュータに無線転送したり、ＬＡＮ(Local Area Network)、インターネットといったネットワークを介して、コンピュータに有線で転送し、コンピュータでは、そのようにして転送されてくるプログラムを受信し、内蔵するハードディスク等の記録媒体にインストールすることができる。

【０２６２】

なお、明細書に記載された各種の処理は、記載に従って時系列に実行されるのみならず、処理を実行する装置の処理能力あるいは必要に応じて並列的にあるいは個別に実行されてもよい。また、本明細書においてシステムとは、複数の装置の論理的集合構成であり、各構成の装置が同一筐体内にあるものには限らない。

【０２６３】

【発明の効果】

以上、説明したように、本発明の構成によれば、暗号化コンテンツの復号に適用する鍵（ブロックキーＫｂ２）を生成するために必要となるシード情報（シード２）を他の鍵（ブロックキーＫｂ１）によって暗号化して格納する構成としたので、シード情報（シード２）をディスクから直接読み取ることは不可能であり、従ってシード情報を用いて生成される鍵情報の解析、暗号アルゴリズムの解析の困難性が高まり、セキュリティレベルの高いコンテンツ保護が実現される。

【０２６４】

さらに、本発明の構成によれば、情報記録媒体に格納されたデータの再生処理において、暗号化コンテンツの復号に適用する鍵（ブロックキーＫｂ２）生成用のシード情報（シード２）をデバイス間で転送することが必要となる構成におい

て、ブロックキー生成情報、具体的には、シード情報（シード２）および記録キーＫ２の双方をセッションキーで暗号化して送受信する構成としたので、転送路からのデータ漏洩が発生した場合であっても、シード情報（シード２）および記録キーＫ２を取得することは困難となり、シード情報を用いて生成される鍵情報の解析、暗号アルゴリズムの解析の困難性が高まり、セキュリティレベルの高いコンテンツ保護が実現される。

【図面の簡単な説明】

【図１】

情報記録媒体に格納されるデータ構成について説明する図である。

【図２】

情報処理装置の構成例について説明する図である。

【図３】

情報処理装置において実行する復号処理について説明する図である。

【図４】

ディスク固有キーの生成処理例について説明する図である。

【図５】

記録キーの生成処理例について説明する図である。

【図６】

記録キーを用いたデータ記録処理について説明する図である。

【図７】

タイトル固有キーの生成処理例について説明する図である。

【図８】

暗号化データの復号処理シーケンスを説明する図である。

【図９】

暗号化データの復号処理シーケンスを説明する図である。

【図１０】

情報記録媒体に格納されるデータ構成について説明する図である。

【図１１】

情報処理装置において実行する復号処理について説明する図である。

【図１２】
暗号化データの復号処理シーケンスを説明する図である。

【図１３】
シード情報の格納構成例について説明する図である。

【図１４】
シード情報の格納構成例について説明する図である。

【図１５】
シード情報の格納構成例について説明する図である。

【図１６】
情報記録媒体ドライブ装置と情報処理装置間の接続構成を説明する図である。

【図１７】
情報記録媒体ドライブ装置と情報処理装置間のデータ転送処理を説明する図である。

【図１８】
情報記録媒体ドライブ装置と情報処理装置間のデータ転送を伴う復号処理シーケンスを説明する図である。

【図１９】
情報記録媒体ドライブ装置と情報処理装置間の認証処理シーケンスを説明する図である。

【図２０】
情報記録媒体ドライブ装置と情報処理装置間のデータ転送を伴う復号処理シーケンスを説明する図である。

【図２１】
情報記録媒体ドライブ装置と情報処理装置間のデータ転送を伴う復号処理シーケンスを説明する図である。

【図２２】
情報記録媒体ドライブ装置と情報処理装置間のデータ転送を伴う復号処理シーケンスを説明する図である。

【図２３】

情報記録媒体ドライブ装置と情報処理装置間のデータ転送を伴う復号処理シーケンスを説明する図である。

【符号の説明】

１００　情報処理装置
１１０　バス
１２０　入出力インタフェース
１３０　ＭＰＥＧコーデック
１４０　入出力インタフェース
１４１　Ａ／Ｄ，Ｄ／Ａコンバータ
１５０　暗号処理手段
１６０　ＲＯＭ
１７０　ＲＡＭ
１８０　メモリ
１９０　記録媒体Ｉ／Ｆ
１９５　記録媒体
１９８　ＴＳ処理手段
２１０　情報処理装置
２１１　マスターキー
２２０　情報記録媒体
２２１　ディスクＩＤ
２２３，２２４　タイトルキー
２２５　記録シード
２２６　物理インデックス
２２７　シード情報
２２８　暗号化コンテンツ
２７１～２７５　暗号処理部
２８１　管理センタ
２８２　コンテンツ編集スタジオ
２８３　ディスク製造エンティティ

２８４　情報記録媒体
２９１，２９２　暗号処理部
２９３，２９５　暗号処理部
２９４　演算部
３００　暗号処理単位
３０１　制御データ
３０２　先頭ＴＳパケット
３０３　後続ＴＳパケット
３０４　復号ＴＳパケット
３０５　復号ＴＳパケット群
３１１　シード情報（シード１）
３１２　シード情報（シード２）
４１０　情報処理装置
４１１　インタフェース
４２０　情報記録媒体ドライブ装置
４２１　インタフェース
４３０　情報記録媒体
５００　情報処理装置
５１０　情報記録媒体ドライブ
５１１　マスターキー
５２０　情報記録媒体
５２１　ディスクＩＤ
５２３，５２４　タイトルキー
５２５　記録シード
５２６　物理インデックス
５２７　シード情報
５２８　暗号化コンテンツ
５３０，５４０　認証キー
６００　暗号処理単位

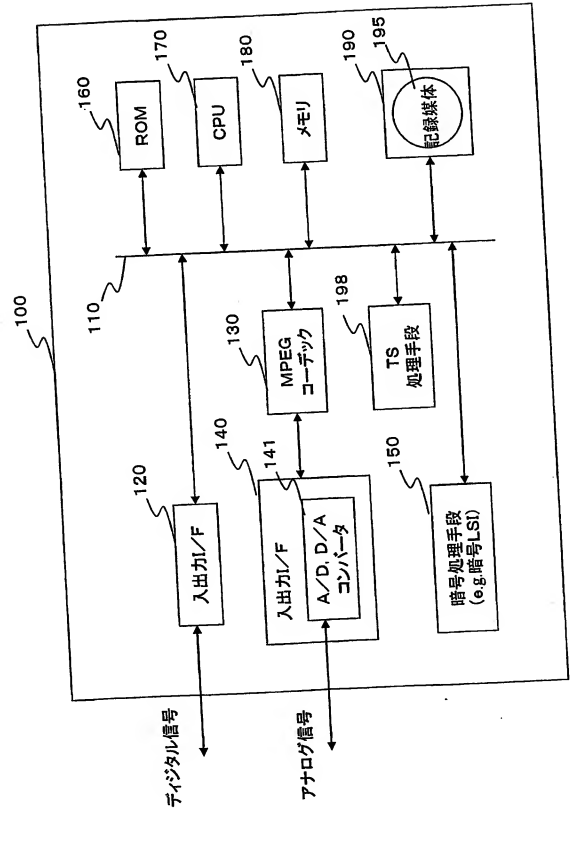
６０１　制御データ
６０２　先頭ＴＳパケット
６０３　後続ＴＳパケット
６０４　復号ＴＳパケット
６０５　暗号化ＴＳパケット
６０６　復号ＴＳパケット
６０７　復号ＴＳパケット群
６１１　シード情報（シード１）
６１２　シード情報（シード２）
６５０　情報処理装置
６６０　情報記録媒体ドライブ
６１１　マスターキー
６７０　情報記録媒体
６７１　ディスクＩＤ
６７２　タイトルキー
６７３　物理インデックス
６７４　シード情報
６７５　暗号化コンテンツ
６８０，６９０　認証キー
７０１　暗号化ユーザデータ
７０２　暗号化ユーザデータ
７０３　ユーザデータ
７１１　制御データ

【書類名】　図面

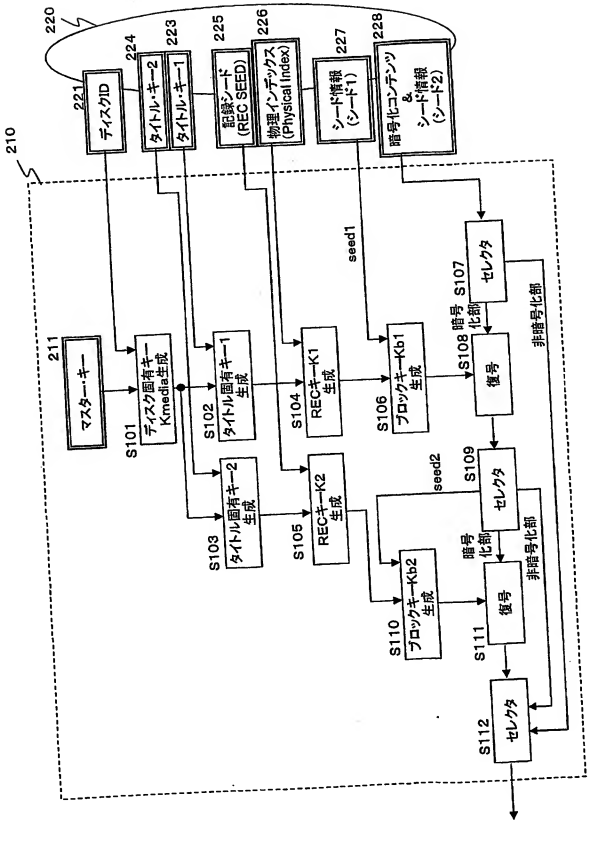
【図１】


(a)記録データ
(b)処理単位
(c)暗号化構成
復号, MPEG復号再生
18B
2048B
制御データ (User Control Data)
User Data
6144B
Seed2(ブロック鍵Kb2の生成に適用)
(ブロック鍵Kb1で暗合化)
ブロック鍵Kb2で暗号化
Seed1(ブロック鍵Kb1の生成に適用)

【図２】


100
110
160
ROM
170
CPU
180
メモリ
190
195
記録媒体
120
入出力I/F
130
MPEG
コーデック
198
TS
処理手段
140
141
入出力I/F
A/D, D/A
コンバータ
150
暗号処理手段
(e.g.暗号LSI)
ディジタル信号
アナログ信号

【図３】


220
221
ディスクID
224
タイトル・キー2
223
タイトル・キー1
225
記録シード (REC SEED)
226
物理インデックス (Physical Index)
227
シード情報 (シード1)
228
暗号化コンテンツ & シード情報 (シード2)
210
211
マスターキー
S101
ディスク固有キー Kmedia生成
S102
タイトル固有キー1 生成
S103
タイトル固有キー2 生成
S104
REC キーK1 生成
S105
REC キーK2 生成
S106
ブロックキーKb1 生成
S107
セレクタ
S108
暗号化部
暗号
非暗号化部
seed1
seed2
S109
セレクタ
暗号化部
暗号
非暗号化部
S110
ブロックキーKb2 生成
S111
復号
S112
セレクタ

【図４】


(a)
ディスクID
AES
ディスク固有キー
マスターキー
(b)
マスターキー||ディスクID
SHA－1
縮約関数
ディスク固有キー

【図５】


(a)
タイトル・キー1
Encrypted
Disc Key 1
(Ked1)
271
AES_D
ディスク固有キー
Media Key
(Kmedia)
タイトル固有キー1
Disc Key 1 (Kd1)
272
AES_E
物理インデックス
(Physical Index)
273
Recording Key (K1)
(b)
タイトル・キー2
Encrypted
Disc Key 2
(Ked2)
274
AES_D
ディスク固有キー
Media Key
(Kmedia)
タイトル固有キー2
Disc Key 2 (Kd2)
記録シード
(Rec Seed)
275
AES_E
Recording Key (K2)

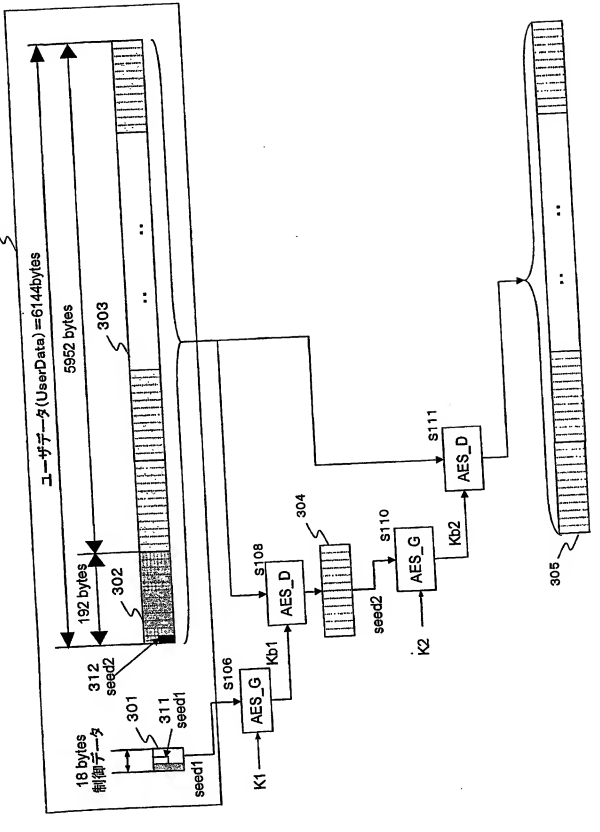
【図６】


281
管理センタ
(TC:Trusted Center)
タイトル固有キー2
取得可能情報
タイトル固有キー1
取得可能情報
282
コンテンツ編集スタジオ
(AS:Authoring Studio)
K2
記録キーK2による
暗号化コンテンツ
283
ディスク製造エンティティ
(DM:Disc Manufacturer)
K1
記録キーK2&K1に
よる暗号化コンテンツ
284

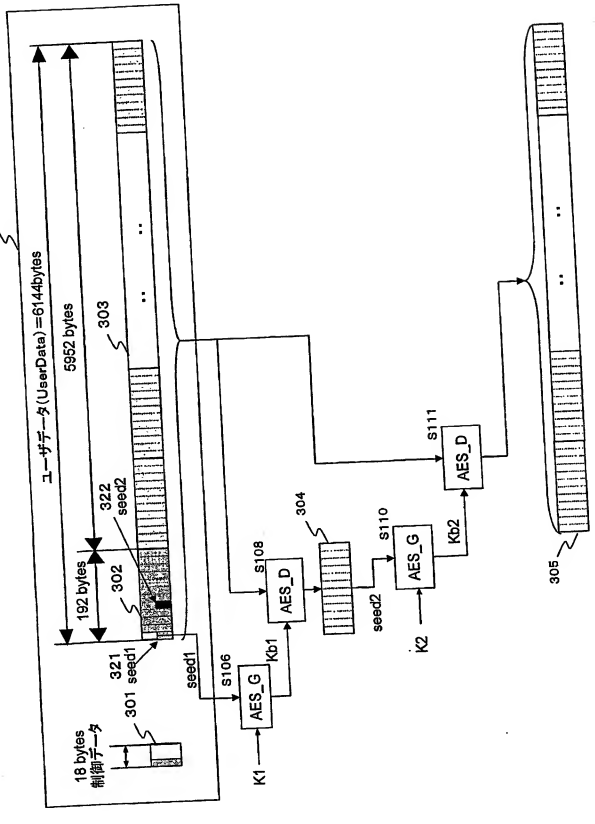
【図７】


(a)出力フィードバックモード
Output Feedback Mode
Disc Key Seed
オーサリング毎にランダムに変わる値
ディスク固有キー
Media Key
(Kmedia)
291
AES_D
タイトル固有キー1
Disc Key 1 (Kd1)
292
AES_D
タイトル固有キー2
Disc Key 2 (Kd2)
(b)カウンタモード
Counter Mode
Disc Key Seed
オーサリング毎にランダムに変わる値
293
AES_D
ディスク固有キー
Media Key
(Kmedia)
タイトル固有キー1
Disc Key 1 (Kd1)
294
(Disc Key Seed +1) mod 2128
295
AES_D
タイトル固有キー2
Disc Key 2 (Kd2)

【図８】


300
ユーザデータ(UserData)=6144bytes
5952 bytes
303
192 bytes
302
312
seed2
301
311
seed1
18 bytes
制御データ
seed1
S106
AES_G
K1
Kb1
S108
AES_D
304
seed2
S110
AES_G
K2
Kb2
S111
AES_D
305

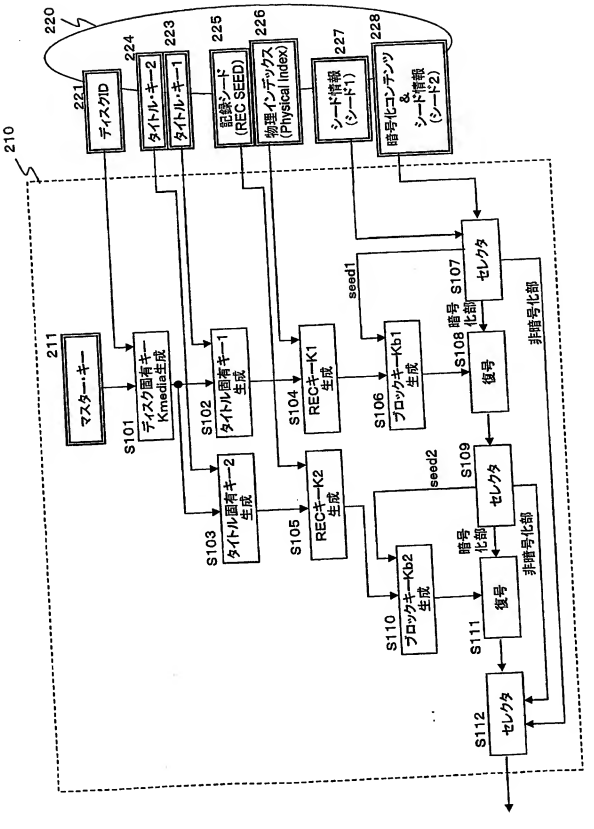
【図９】


300
ユーザデータ(UserData)＝6144bytes
5952 bytes
192 bytes
303
322
seed2
302
321
seed1
301
18 bytes
制御データ
seed1
S106
AES_G
K1
Kb1
S108
AES_D
304
seed2
S110
AES_G
K2
Kb2
S111
AES_D
305

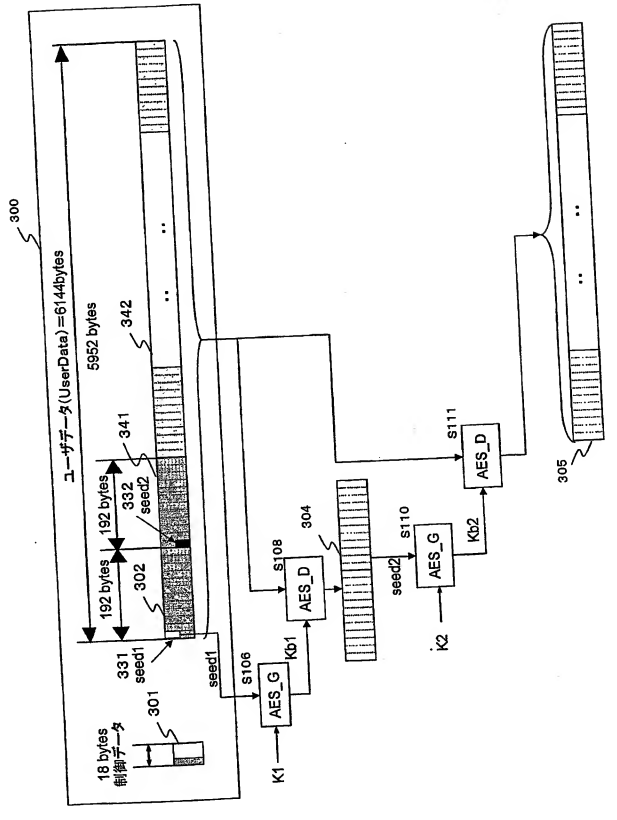
【図１０】


(a) 暗号化処理単位の先頭192byte(ヘッダ部＋1TSパケット)
192 bytes
TSパケット(188bytes)
ヘッダ部
(4bytes)
seed1
(b) 暗号化処理単位の先頭4byte(ヘッダ部のみ)
31
0
CCI
ATS
CCI 2bit
ATS 30bit

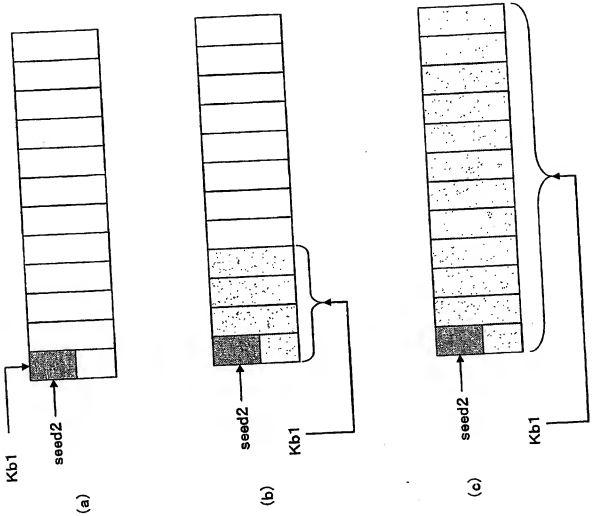
【図１１】


220
210
221
ディスクID
224
タイトルキー2
223
タイトルキー1
225
記録シード
(REC SEED)
226
物理インデックス
(Physical Index)
227
シード情報
(シード1)
228
暗号化コンテンツ
&
シード情報
(シード2)
211
マスターキー
S101
ディスク固有キー
Kmedia生成
S102
タイトル固有キー1
生成
S103
タイトル固有キー2
生成
S104
RECキーK1
生成
S105
RECキーK2
生成
S106
ブロックキーKb1
生成
S107
セレクタ
S108
暗号
化部
復号
非暗号化部
seed1
S109
セレクタ
暗号
化部
復号
非暗号化部
seed2
S110
ブロックキーKb2
生成
S111
セレクタ
非暗号化部
S112
セレクタ

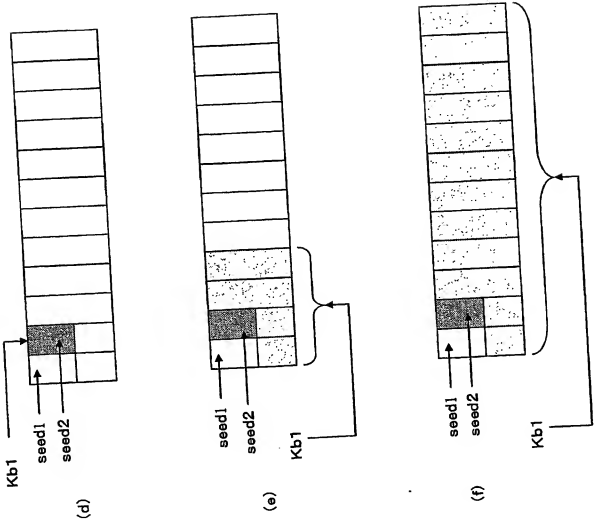
【図１２】


300
ユーザデータ(UserData)＝6144bytes
5952 bytes
342
192 bytes
341
192 bytes
332
seed2
192 bytes
302
331
seed1
301
18 bytes
制御データ
seed1
S106
AES_G
K1
Kb1
S108
AES_D
304
seed2
S110
AES_G
K2
Kb2
S111
AES_D
305

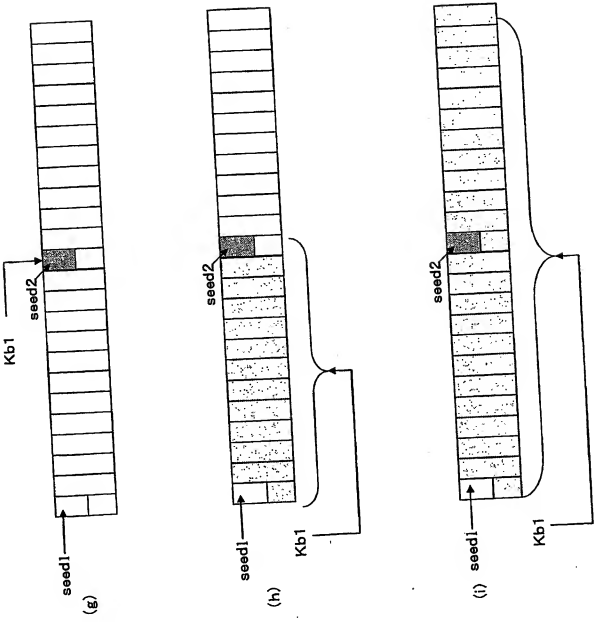
【図１３】



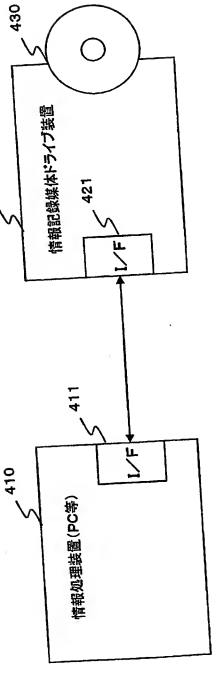
【図１４】



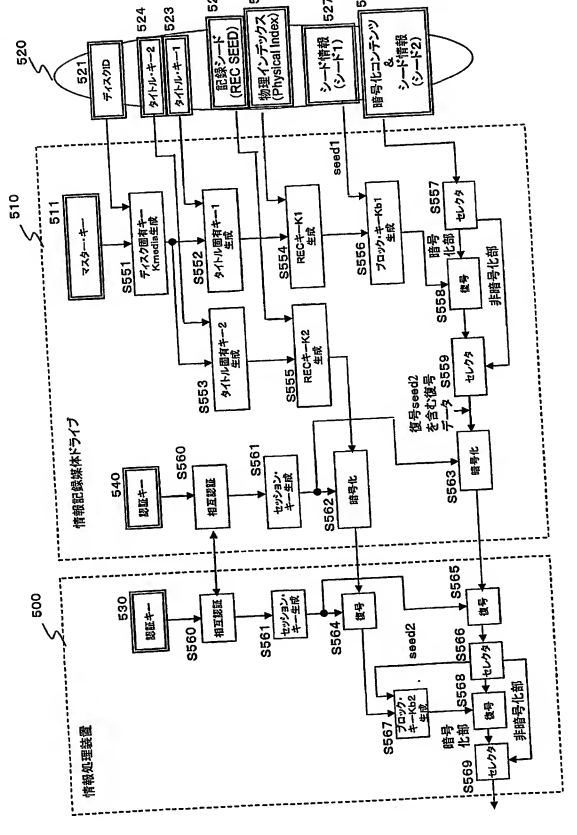
【図１５】



【図１６】



【図１７】


500
情報処理装置
510
情報記録媒体ドライブ
520
521 ディスクID
524 タイトル・キー2
523 タイトル・キー1
525 記録シード (REC SEED)
526 物理インデックス (Physical Index)
527 シード情報 (シード1)
528 暗号化コンテンツ & シード情報 (シード2)
511 マスター・キー
530 認証キー
540 認証キー
S551 ディスク個有キー Kmedia生成
S552 タイトル個有キー1 生成
S553 タイトル個有キー2 生成
S554 REC-K1 生成
S555 REC-K2 生成
S556 ブロック・キー-Ko1 生成
S557 セレクタ
S558 暗号化部
S559 セレクタ
S560 相互認証
S561 セッション・キー生成
S562 暗号化
S563 暗号化
S564 復号
S565 復号
S566 セレクタ
S567 ブロック・キー-Ko2 生成
S568 暗号化部
S569 セレクタ
seed1
seed2
復号seed2を含む復号データ
暗号化部
非暗号化部
復号
セレクタ

【図１８】


600
ユーザデータ(UserData)=6144bytes
5952 bytes
603
192 bytes
602
612
seed2
601
611
seed1
18 bytes
制御データ
S556
AES_G
Kb1
K1
S558
AES_D
604
S563
AES_E
605
S565
AES_D
606
S567
AES_G
Kb2
S568
AES_D
607
記録キー
K2
S562
AES_E
Ks
S564
AES_D
Ks
K2
seed2
seed1
ドライブ
通信路
情報処理装置

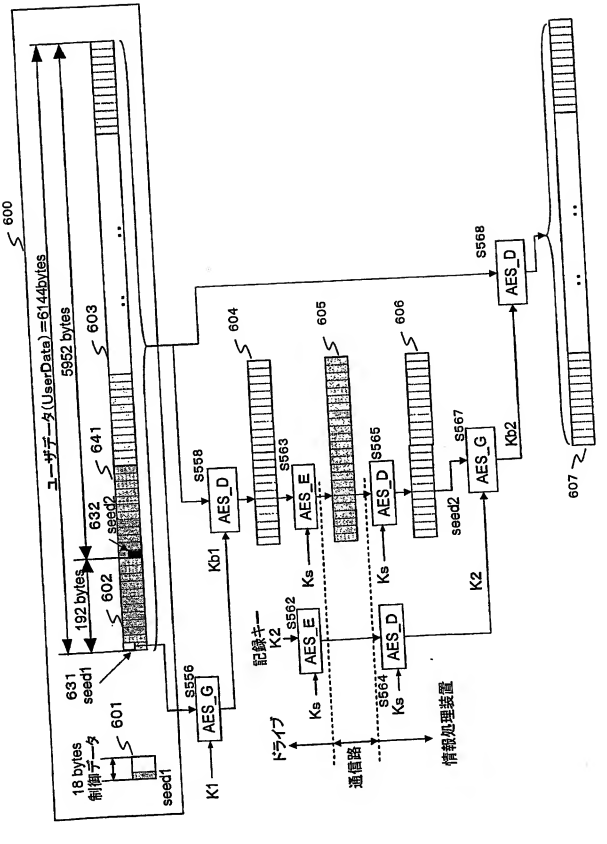
【図１９】


500
情報処理装置
530
共有認証キーKm
Km
S571
乱数Rb1生成
S572
MAC (AES)
S573
比較
S574
乱数Rb2生成
S575
MAC (AES)
S576
乱数Rb3生成
S577
セッションキーKs生成
Session Key Ks = eKm(Ra3 || Rb3) 128bits
Rb1 64bits
eKm(Ra1 || Rb1) 128bits
Ra1 64bits
Rb2 64bits
eKm(Rb2 || Ra2) 128bits
Ra2 64bits
Rb3 64bits
Ra3 64bits
510
情報記録媒体ドライブ
540
共有認証キーKm
Km
S582
MAC (AES)
S581
乱数Ra1生成
S585
比較
S584
MAC (AES)
S583
乱数Ra2生成
S587
セッションキーKs生成
S586
乱数Ra3生成
Session Key Ks = eKm(Ra3 || Rb3) 128bits

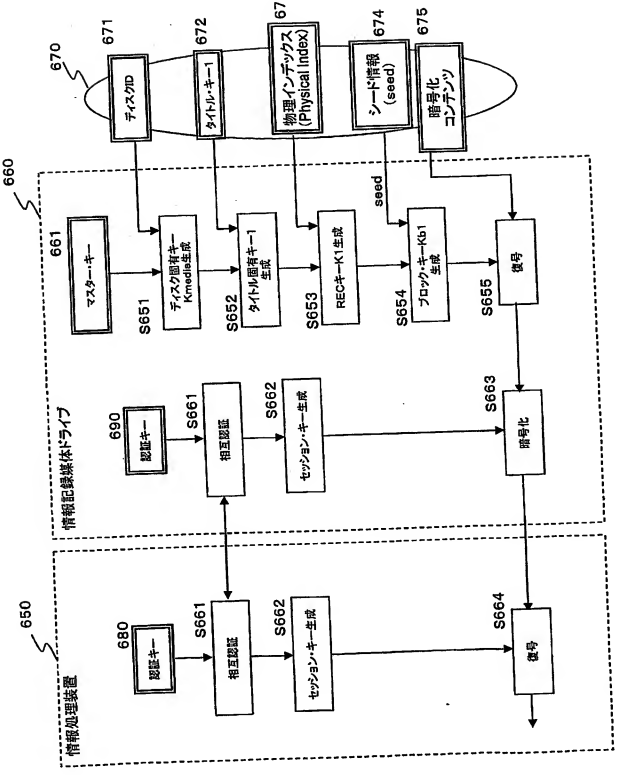
【図２０】


600
ユーザデータ(UserData)=6144bytes
5952 bytes
603
192 bytes
622
seed2
602
621
seed1
601
18 bytes
制御データ
seed1
S556
AES_G
K1
Kb1
S558
AES_D
604
S563
AES_E
605
記録キー
K2
S562
AES_E
Ks
ドライブ
通信路
S564
AES_D
Ks
Ks
AES_D
S565
606
seed2
S567
AES_G
K2
Kb2
S568
AES_D
情報処理装置
607

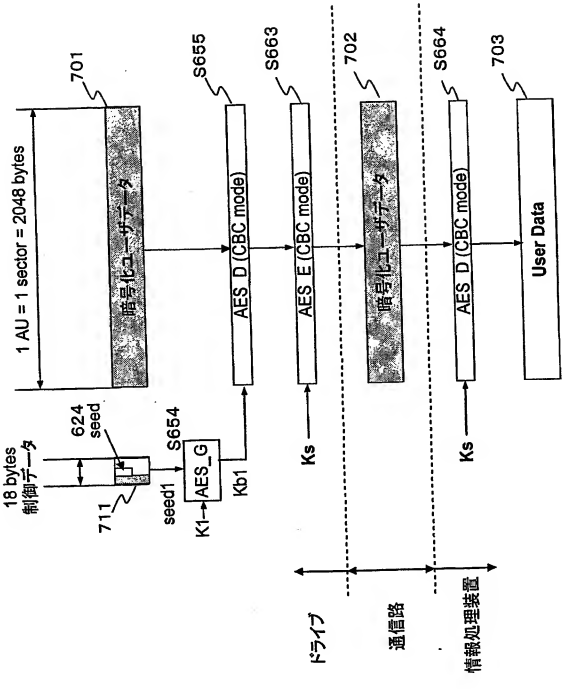
【図２１】


600
ユーザデータ(UserData)=6144bytes
5952 bytes
192 bytes
18 bytes
制御データ
601
602
603
631
seed1
632
seed2
641
seed1
seed2
S556
S558
S562
S563
S564
S565
S567
S568
AES_G
AES_D
AES_E
K1
Kb1
K2
Kb2
Ks
記録キー
ドライブ
通信路
情報処理装置
604
605
606
607

【図２２】


650
情報処理装置
680
認証キー
S661
相互認証
S662
セッション・キー生成
S664
復号
660
情報記録媒体ドライブ
690
認証キー
S661
相互認証
S662
セッション・キー生成
S663
暗号化
661
マスター・キー
S651
ディスク固有キー Kmedia生成
S652
タイトル固有キー生成
S653
REC キー K1生成
S654
ブロック・キー Kb1 生成
S655
復号
seed
670
671
ディスクID
672
タイトル・キー
673
物理インデックス (Physical Index)
674
シード情報 (seed)
675
暗号化コンテンツ

【図２３】


1 AU = 1 sector = 2048 bytes
701
暗号化ユーザデータ
S655
AES_D (CBC mode)
S663
AES_E (CBC mode)
702
暗号化ユーザデータ
S664
AES_D (CBC mode)
703
User Data
18 bytes
制御データ
624
seed
711
S654
seed1
K1→AES_G
Kb1
Ks
Ks
ドライブ
通信路
情報処理装置

【書類名】　要約書

【要約】

【課題】　情報記録媒体に格納される暗号化コンテンツの不正利用を効果的に防止することを可能とした構成を提供する。

【解決手段】　暗号化コンテンツの復号に適用するブロックキーを生成するために必要となるシード情報（シード２）をブロックキーＫｂ１によって暗号化して格納する構成とした。さらに、シード情報（シード２）をデバイス間で転送することが必要となる構成において、シード情報（シード２）および記録キーＫ２の双方をセッションキーで暗号化して送受信する構成とした。本構成により、情報記録媒体、およびデータ転送路からのデータ取得によるシード情報（シード２）解析は困難となり、シード情報を用いて生成される鍵情報の解析、暗号アルゴリズムの解析困難性を向上させたセキュリティレベルの高いコンテンツ保護が実現される。

【選択図】　図８

特願２００３－１０７５７１

出 願 人 履 歴 情 報

識別番号 [０００００２１８５]

１．変更年月日 １９９０年 ８月３０日
[変更理由] 新規登録
住 所 東京都品川区北品川６丁目７番３５号
氏 名 ソニー株式会社